

Virtual Private Cloud

API Reference

Issue	01
Date	2025-08-19



Copyright © Huawei Technologies Co., Ltd. 2025. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks 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 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.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: <https://www.huawei.com>

Email: support@huawei.com

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:

<https://www.huawei.com/en/psirt/vul-response-process>

For vulnerability information, enterprise customers can visit the following web page:

<https://securitybulletin.huawei.com/enterprise/en/security-advisory>

Contents

1 Before You Start.....	1
2 API Overview.....	4
3 Calling APIs.....	6
3.1 Making an API Request.....	6
3.2 Authentication.....	10
3.3 Response.....	11
4 VPC APIs (V1/V2).....	14
4.1 Virtual Private Cloud.....	14
4.1.1 Creating a VPC.....	14
4.1.2 Querying VPC Details.....	18
4.1.3 Querying VPCs.....	21
4.1.4 Updating a VPC.....	26
4.1.5 Deleting a VPC.....	30
4.2 Subnet.....	31
4.2.1 Creating a Subnet.....	31
4.2.2 Querying Subnet Details.....	44
4.2.3 Querying Subnets.....	50
4.2.4 Updating Subnet Information.....	57
4.2.5 Deleting a Subnet.....	63
4.3 Quota.....	64
4.3.1 Querying Quotas.....	65
4.4 Private IP Address.....	70
4.4.1 Assigning a Private IP Address.....	71
4.4.2 Querying Private IP Address Details.....	74
4.4.3 Querying Private IP Addresses.....	77
4.4.4 Deleting a Private IP Address.....	81
4.5 Security Group.....	82
4.5.1 Creating a Security Group.....	82
4.5.2 Querying Security Group Details.....	88
4.5.3 Querying Security Groups.....	93
4.5.4 Deleting a Security Group.....	101
4.5.5 Adding a Security Group Rule.....	102

4.5.6 Querying Security Group Rule Details.....	107
4.5.7 Querying Security Group Rules.....	111
4.5.8 Deleting a Security Group Rule.....	117
4.6 Port.....	117
4.6.1 Creating a Port.....	118
4.6.2 Querying a Port.....	130
4.6.3 Querying Ports.....	138
4.6.4 Updating a Port.....	150
4.6.5 Deleting a Port.....	162
4.7 VPC Peering Connection.....	163
4.7.1 Querying VPC Peering Connections.....	163
4.7.2 Querying a VPC Peering Connection.....	168
4.7.3 Creating a VPC Peering Connection.....	170
4.7.4 Accepting a VPC Peering Connection.....	174
4.7.5 Refusing a VPC Peering Connection.....	176
4.7.6 Updating a VPC Peering Connection.....	178
4.7.7 Deleting a VPC Peering Connection.....	181
4.8 VPC Route.....	182
4.8.1 Querying VPC Routes.....	182
4.8.2 Querying a VPC Route.....	186
4.8.3 Creating a VPC Route.....	188
4.8.4 Deleting a VPC Route.....	190
4.9 Route Table.....	191
4.9.1 Querying Route Tables.....	191
4.9.2 Querying a Route Table.....	195
4.9.3 Creating a Route Table.....	199
4.9.4 Updating a Route Table.....	207
4.9.5 Associating Subnets with a Route Table.....	221
4.9.6 Disassociating Subnets from a Route Table.....	226
4.9.7 Deleting a Route Table.....	231
4.10 VPC Tag Management.....	232
4.10.1 Adding a Tag to a VPC.....	232
4.10.2 Querying VPC Tags.....	234
4.10.3 Deleting a Tag from a VPC.....	236
4.10.4 Batch Adding or Deleting VPC Tags.....	237
4.10.5 Querying VPCs by Tag.....	239
4.10.6 Querying VPC Tags in a Specified Project.....	244
4.11 Subnet Tag Management.....	246
4.11.1 Adding a Tag to a Subnet.....	246
4.11.2 Querying Subnet Tags.....	248
4.11.3 Deleting a Tag from a Subnet.....	250
4.11.4 Batch Adding or Deleting Subnet Tags.....	251

4.11.5 Querying Subnets by Tag..... 253

4.11.6 Querying Subnet Tags in a Specified Project..... 258

4.12 Security Group Tag Management..... 260

4.12.1 Querying Security Groups by Tag..... 260

4.12.2 Batch Adding Tags to a Security Group..... 266

4.12.3 Batch Deleting Tags from a Security Group..... 269

4.12.4 Querying Security Group Tags..... 273

4.12.5 Adding a Tag to a Security Group..... 276

4.12.6 Deleting a Tag from a Security Group..... 279

4.12.7 Querying Security Group Tags in a Specified Project..... 282

4.13 Querying IP Address Usage..... 285

4.13.1 Querying IP Address Usage on a Specified Network..... 285

4.14 VPC Flow Log..... 288

4.14.1 Creating a VPC Flow Log..... 288

4.14.2 Querying VPC Flow Logs..... 292

4.14.3 Querying a VPC Flow Log..... 298

4.14.4 Updating a VPC Flow Log..... 301

4.14.5 Deleting a VPC Flow Log..... 304

5 VPC APIs (V3)..... 306

5.1 VPC..... 306

5.1.1 Querying VPCs..... 306

5.1.2 Querying the Details of a VPC..... 316

5.1.3 Adding a Secondary CIDR Block to a VPC..... 323

5.1.4 Removing a Secondary CIDR Block from a VPC..... 335

5.2 Security Group..... 346

5.2.1 Creating a Security Group..... 347

5.2.2 Querying Security Groups..... 363

5.2.3 Querying the Details of a Security Group..... 371

5.2.4 Updating a Security Group..... 381

5.2.5 Deleting a Security Group..... 393

5.3 Security Group Rule..... 397

5.3.1 Creating a Security Group Rule..... 397

5.3.2 Querying a Security Group Rule..... 410

5.3.3 Querying Security Group Rules..... 417

5.3.4 Deleting a Security Group Rule..... 427

5.3.5 Adding Rules to a Specified Security Group..... 430

5.4 IP Address Group..... 445

5.4.1 Creating an IP Address Group..... 445

5.4.2 Querying IP Address Groups..... 460

5.4.3 Querying an IP Address Group..... 471

5.4.4 Updating an IP Address Group..... 479

5.4.5 Deleting an IP Address Group..... 493

5.4.6 Forcibly Deleting an IP Address Group.....	496
5.5 Supplementary Network Interface.....	500
5.5.1 Creating a Supplementary Network Interface.....	500
5.5.2 Creating Supplementary Network Interfaces in Batches.....	516
5.5.3 Querying Supplementary Network Interfaces.....	532
5.5.4 Querying the Details of a Supplementary Network Interface.....	548
5.5.5 Querying the Number of Supplementary Network Interfaces.....	557
5.5.6 Updating a Supplementary Network Interface.....	561
5.5.7 Deleting a Supplementary Network Interface.....	576
5.6 Traffic Mirror Sessions.....	579
5.6.1 Querying Traffic Mirror Sessions.....	579
5.6.2 Querying Details About a Traffic Mirror Session.....	589
5.6.3 Creating a Traffic Mirror Session.....	596
5.6.4 Updating a Traffic Mirror Session.....	606
5.6.5 Deleting a Traffic Mirror Session.....	614
5.6.6 Disassociating a Traffic Mirror Source from a Traffic Mirror Session.....	618
5.6.7 Associating a Traffic Mirror Source with a Traffic Mirror Session.....	626
5.7 Traffic Mirror Filters.....	634
5.7.1 Creating a Traffic Mirror Filter.....	634
5.7.2 Querying Traffic Mirror Filters.....	644
5.7.3 Querying Details About a Traffic Mirror Filter.....	654
5.7.4 Updating a Traffic Mirror Filter.....	664
5.7.5 Deleting a Traffic Mirror Filter.....	673
5.8 Traffic Mirror Filter Rules.....	677
5.8.1 Querying Traffic Mirror Filter Rules.....	677
5.8.2 Querying Details About a Traffic Mirror Filter Rule.....	688
5.8.3 Creating a Traffic Mirror Filter Rule.....	697
5.8.4 Updating a Traffic Mirror Filter Rule.....	707
5.8.5 Deleting a Traffic Mirror Filter Rule.....	716
5.9 Network ACL.....	719
5.9.1 Creating a Network ACL.....	719
5.9.2 Querying Network ACLs.....	729
5.9.3 Querying the Details of a Network ACL.....	736
5.9.4 Updating a Network ACL.....	744
5.9.5 Deleting a Network ACL.....	754
5.9.6 Updating a Network ACL Rule.....	757
5.9.7 Inserting a Network ACL Rule.....	770
5.9.8 Deleting a Network ACL Rule.....	785
5.9.9 Associating a Subnet with a Network ACL.....	795
5.9.10 Disassociating a Subnet from a Network ACL.....	803
5.10 Network ACL Tag Management.....	813
5.10.1 Querying the Number of Network ACLs Using Tags.....	813

5.10.2 Querying Network ACLs Using Tags.....	819
5.10.3 Adding a Tag to a Network ACL.....	826
5.10.4 Deleting a Tag from a Network ACL.....	831
5.10.5 Querying Tags of a Network ACL.....	834
5.10.6 Adding Tags to a Network ACL in Batches.....	838
5.10.7 Deleting Tags from a Network ACL in Batches.....	843
5.10.8 Querying Tags of Network ACLs in a Project.....	848
5.11 Port.....	852
5.11.1 Adding a Security Group to the Security Group List of a Port.....	853
5.11.2 Removing a Security Group from the Security Group List of a Port.....	863
5.12 Subnet CIDR Reservations.....	873
5.12.1 Creating a Subnet CIDR Reservation.....	873
5.12.2 Querying the List of Subnet CIDR Reservations.....	879
5.12.3 Querying Details About a Subnet CIDR Reservation.....	884
5.12.4 Updating a Subnet CIDR Reservation.....	887
5.12.5 Deleting a Subnet CIDR Reservation.....	891
6 Native OpenStack Neutron APIs (V2.0).....	893
6.1 API Version Information.....	893
6.1.1 Querying API Versions.....	893
6.1.2 Pagination.....	895
6.2 Port.....	897
6.2.1 Querying Ports.....	898
6.2.2 Querying a Port.....	916
6.2.3 Creating a Port.....	926
6.2.4 Updating a Port.....	940
6.2.5 Deleting a Port.....	954
6.3 Network.....	955
6.3.1 Querying Networks.....	955
6.3.2 Querying Network Details.....	961
6.3.3 Creating a Network.....	964
6.3.4 Updating a Network.....	968
6.3.5 Deleting a Network.....	972
6.4 Subnet.....	972
6.4.1 Querying Subnets.....	973
6.4.2 Querying a Subnet.....	979
6.4.3 Creating a Subnet.....	983
6.4.4 Updating a Subnet.....	991
6.4.5 Deleting a Subnet.....	998
6.5 Router.....	999
6.5.1 Querying Routers.....	999
6.5.2 Querying a Router.....	1003
6.5.3 Creating a Router.....	1006

6.5.4 Updating a Router.....	1009
6.5.5 Deleting a Router.....	1013
6.5.6 Adding an Interface to a Router.....	1014
6.5.7 Removing an Interface from a Router.....	1015
6.6 Network ACL.....	1017
6.6.1 Querying Network ACL Rules.....	1017
6.6.2 Querying a Network ACL Rule.....	1021
6.6.3 Creating a Network ACL Rule.....	1023
6.6.4 Updating a Network ACL Rule.....	1027
6.6.5 Deleting a Network ACL Rule.....	1030
6.6.6 Querying Network ACL Policies.....	1031
6.6.7 Querying a Network ACL Policy.....	1036
6.6.8 Creating a Network ACL Policy.....	1037
6.6.9 Updating a Network ACL Policy.....	1040
6.6.10 Deleting a Network ACL Policy.....	1042
6.6.11 Inserting a Network ACL Rule.....	1043
6.6.12 Removing a Network ACL Rule.....	1045
6.6.13 Querying Network ACL Groups.....	1047
6.6.14 Querying a Network ACL Group.....	1052
6.6.15 Creating a Network ACL Group.....	1054
6.6.16 Updating a Network ACL Group.....	1058
6.6.17 Deleting a Network ACL Group.....	1061
6.7 Security Group.....	1062
6.7.1 Querying Security Groups.....	1062
6.7.2 Querying a Security Group.....	1067
6.7.3 Creating a Security Group.....	1071
6.7.4 Updating a Security Group.....	1075
6.7.5 Deleting a Security Group.....	1079
6.7.6 Querying Security Group Rules.....	1079
6.7.7 Querying a Security Group Rule.....	1085
6.7.8 Adding a Security Group Rule.....	1088
6.7.9 Deleting a Security Group Rule.....	1093
7 Application Examples.....	1094
7.1 Example 1: Creating a VPC and Subnet for an ECS.....	1094
7.2 Example 2: Configuring a Security Group for an ECS.....	1096
7.3 Example 3: Assigning a Virtual IP Address to an ECS for HA.....	1099
7.4 Example 4: Assigning a Virtual IPv6 Address to ECSs for HA.....	1103
8 Permissions and Supported Actions.....	1108
8.1 Introduction.....	1108
8.2 Permissions and Supported Actions of API V1 and V2.....	1109
8.2.1 VPC.....	1109
8.2.2 Subnet.....	1109

8.2.3 Port.....	1110
8.2.4 VPC Peering Connection.....	1110
8.2.5 VPC Route.....	1111
8.2.6 Route Table.....	1111
8.2.7 Quota.....	1112
8.2.8 Private IP Address.....	1112
8.2.9 Security Group.....	1112
8.2.10 Security Group Rule.....	1113
8.2.11 VPC Tag.....	1113
8.2.12 Subnet Tag.....	1114
8.2.13 VPC Flow Log.....	1114
8.3 Permissions and Supported Actions of Native OpenStack Neutron V2.0.....	1114
8.3.1 Port (OpenStack Neutron API).....	1115
8.3.2 Network (OpenStack Neutron API).....	1115
8.3.3 Subnet (OpenStack Neutron API).....	1115
8.3.4 Router (OpenStack Neutron API).....	1116
8.3.5 Network ACL (OpenStack Neutron API).....	1116
8.3.6 Security Group (OpenStack Neutron API).....	1118
8.4 Permissions and Supported Actions of API V3.....	1119
8.4.1 VPC (V3).....	1119
8.4.2 Security Group (V3).....	1119
8.4.3 Security Group Rule (V3).....	1120
8.4.4 IP Address Group (V3).....	1120
8.4.5 Supplementary Network Interface (V3).....	1121
8.4.6 Mirror Session (V3).....	1121
8.4.7 Mirror Filter (V3).....	1122
8.4.8 Mirror Filter Rule (V3).....	1123
8.4.9 Network ACL (V3).....	1123
8.4.10 Network ACL Tag (V3).....	1124
8.4.11 Port (V3).....	1125
8.5 Precautions for API Permissions.....	1125
9 FAQs.....	1127
9.1 What Are the Differences Between the VPC Subnet API and the OpenStack Neutron Subnet API?.....	1127
9.2 What Are the Relationships Among Network ACL Groups, Policies, and Rules?.....	1129
10 Out-of-Date APIs.....	1132
10.1 Port (Discarded).....	1132
10.1.1 Creating a Port (Discarded).....	1132
10.1.2 Querying a Port (Discarded).....	1140
10.1.3 Querying Ports (Discarded).....	1146
10.1.4 Updating a Port (Discarded).....	1154
10.1.5 Deleting a Port (Discarded).....	1162

A Appendix..... 1164

A.1 ICMP-Port Range Relationship Table..... 1164

A.2 VPC Monitoring Metrics..... 1165

A.3 Status Codes..... 1167

A.4 Error Codes..... 1168

A.5 Obtaining a Project ID..... 1196

1 Before You Start

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

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](#).

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](#).

You need to select an endpoint based on your service requirements.

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](#).

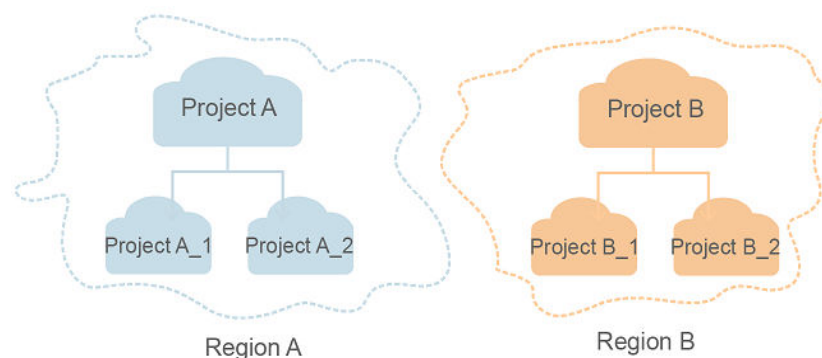
- AZ

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](#).

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 Flow logs are available only in certain regions. For details, visit Function Overview and click Flow Log .

VPC v3 APIs

Table 2-2 API description

Type	Description
VPC V3	APIs for querying and editing secondary CIDR blocks.
Security Group (V3)	APIs for creating, querying, updating, and deleting security groups.
Security Group Rule (V3)	APIs for adding, querying, and deleting security group rules.
IP Address Group	APIs for creating, querying, updating, and deleting IP address groups.
Supplementary Network Interface	- APIs for creating, querying, updating, and deleting supplementary network interfaces. - Network interfaces are available only in certain regions. For details, visit Function Overview and click Elastic Network Interface.
Network ACL (V3)	APIs for creating, querying, updating, and deleting network ACLs.
Port (V3)	APIs for adding a port to or removing a port from a security group.

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.

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 .
query-string	Query parameter, which is optional. Ensure that a question mark (?) is included before each query parameter that is in the format of <i>Parameter name=Parameter value</i> . 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.
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 <i>Hostname:Port number</i> . 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
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

Parameter	Description	Mandatory	Example Value
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: MIIPAgYJKoZlhvcNAQcCo...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.

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 a 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": "xxxxxxx" // 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:

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

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.
- The AK/SK can either be permanent or temporary. If it is temporary, the **X-Security-Token** field must be included in the request header. The value is the security token of the temporary AK/SK.

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_ 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 shows 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 VPC APIs (V1/V2)

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. - Range: 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. - Range: 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. - Range: 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: <i>yyyy-MM-ddTHH:mm:ss</i>

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

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. - Range: 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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	- Specifies the time (UTC) when the VPC is updated. - Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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, 11th to 2,000th resource records will be returned. The default value of limit is 2000.
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. - Range: 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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	- Specifies the time (UTC) when the VPC is updated. - Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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. - Range: 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. - Range: 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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	- Specifies the time (UTC) when the VPC is updated. - Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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.

Parameter	Mandatory	Type	Description
availability_zone	No	String	- Identifies the AZ that the subnet belongs to, which can be obtained from endpoints. For details, see Endpoints. - The value of this parameter is the AZ specified when the subnet is created and does not limit the usage scope of the subnet. If this parameter is not specified, the value will be left blank.
vpc_id	Yes	String	Specifies the ID of the VPC that the subnet belongs to.
extra_dhcp_options	No	Array of extra_dhcp_options 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 domain name, or DHCP lease expiration time configured for the subnet. - Constraints: - If opt_name is set to ntp, the value 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 (.). If opt_name is set to null, the value indicates that no NTP server is configured for the subnet. The parameter value cannot be an empty string. - If opt_name is set to domainname, the value is the domain name configured for DNS and is used to obtain the IP address from the DNS server. A domain name can contain only letters, digits, and hyphens (-) and cannot start or end with a hyphen (-). Each domain name contains at least two labels separated by periods (.). Max total: 254 characters. Max label: 63 characters. - The option addresstime for opt_name indicates the DHCP lease expiration time of the IPv4 subnet. The value can be -1, which indicates unlimited lease time, or Numberh. The number ranges from 1 to 175200. For example, the value can be 5h. The default value is 87600h. - The option ipv6_addresstime for opt_name indicates the DHCP lease expiration time of the IPv6 subnet. The value can be -1, which indicates unlimited

Parameter	Mandatory	Type	Description
			lease time, or <i>Numberh</i> . The number ranges from 1 to 175200 . For example, the value can be 5h . The default value is 2h .
opt_name	Yes	String	- Specifies the NTP server address or DHCP lease expiration time configured for the subnet. - Currently, the value can be ntp, domainname, addresstime, or ipv6_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"
      },
      {
        "opt_value": "24h",
        "opt_name": "addresstime"
      },
      {
        "opt_value": "2h",
        "opt_name": "ipv6_addresstime"
      }
    ]
  }
}
```


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.
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.

Parameter	Type	Description
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.
availability_zone	String	- Identifies the AZ that the subnet belongs to, which can be obtained from endpoints. For details, see Endpoints. - The value of this parameter is the AZ specified when the subnet is created and does not limit the usage scope of the subnet. If this parameter is not specified, the value will be left blank.
vpc_id	String	Specifies the ID of the VPC that the subnet belongs to.

Parameter	Type	Description
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.
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 .

Parameter	Type	Description
scope	String	- Specifies where the subnet is used in edge cloud scenario. - Range: center: The subnet is used in a central AZ. <i>{publicBorderGroup}</i>: The subnet is used in a public border group. The public border group limits the usage scope of a subnet but can have multiple edge AZs associated. You can obtain the AZs by the API for Listing AZs.
tenant_id	String	Project ID
created_at	String	- Specifies the time (UTC) when the subnet is created. - Format: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	- Specifies the time (UTC) when the subnet is updated. - Format: <i>yyyy-MM-ddTHH:mm:ss</i>

Table 4-29 extra_dhcp_opt object

Parameter	Mandatory	Type	Description
opt_value	No	String	- Specifies the NTP server address domain name, or DHCP lease expiration time configured for the subnet. - Constraints: - If opt_name is set to ntp, the value 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 (.). If opt_name is set to null, the value indicates that no NTP server is configured for the subnet. The parameter value cannot be an empty string. - If opt_name is set to domainname, the value is the domain name configured for DNS and is used to obtain the IP address from the DNS server. A domain name can contain only letters, digits, and hyphens (-) and cannot start or end with a hyphen (-). Each domain name contains at least two labels separated by periods (.). Max total: 254 characters. Max label: 63 characters. - The option addresstime for opt_name indicates the DHCP lease expiration time of the IPv4 subnet. The value can be -1, which indicates unlimited lease time, or Numberh. The number ranges from 1 to 175200. For example, the value can be 5h. The default value is 87600h. - The option ipv6_addresstime for opt_name indicates the DHCP lease expiration time of the IPv6 subnet. The value can be -1, which indicates unlimited

Parameter	Mandator y	Type	Description
			lease time, or <i>Numberh</i> . The number ranges from 1 to 175200 . For example, the value can be 5h . The default value is 2h .
opt_name	Yes	String	- Specifies the NTP server address or DHCP lease expiration time configured for the subnet. - Currently, the value can be ntp, domainname, addresstime, or ipv6_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"
      },
      {
        "opt_value": "24h",
        "opt_name": "addresstime"
      },
      {
        "opt_value": "2h",
        "opt_name": "ipv6_addresstime"
      }
    ],
    "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 .
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.
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.

Parameter	Type	Description
availability_zone	String	Identifies the AZ that the subnet belongs to. The value of this parameter is the AZ specified when the subnet is created and does not limit the usage scope of the subnet.
vpc_id	String	Specifies the ID of the VPC that the subnet belongs to.
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_option objects	Specifies the NTP server address or DHCP lease time configured for the subnet. For details, see Table 4-33 .
scope	String	- Specifies where the subnet is used in edge cloud scenario. - Range: center: The subnet is used in a central AZ. <i>{publicBorderGroup}</i>: The subnet is used in a public border group. The public border group limits the usage scope of a subnet but can have multiple edge AZs associated. You can obtain the AZs by the API for Listing AZs.
tenant_id	String	Project ID

Parameter	Type	Description
created_at	String	- Specifies the time (UTC) when the subnet is created. - Format: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	- Specifies the time (UTC) when the subnet is updated. - Format: <i>yyyy-MM-ddTHH:mm:ss</i>

Table 4-33 extra_dhcp_opt object

Parameter	Mandatory	Type	Description
opt_value	No	String	- Specifies the NTP server address domain name, or DHCP lease expiration time configured for the subnet. - Constraints: - If opt_name is set to ntp, the value 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 (.). If opt_name is set to null, the value indicates that no NTP server is configured for the subnet. The parameter value cannot be an empty string. - If opt_name is set to domainname, the value is the domain name configured for DNS and is used to obtain the IP address from the DNS server. A domain name can contain only letters, digits, and hyphens (-) and cannot start or end with a hyphen (-). Each domain name contains at least two labels separated by periods (.). Max total: 254 characters. Max label: 63 characters. - The option addresstime for opt_name indicates the DHCP lease expiration time of the IPv4 subnet. The value can be -1, which indicates unlimited lease time, or Numberh. The number ranges from 1 to 175200. For example, the value can be 5h. The default value is 87600h. - The option ipv6_addresstime for opt_name indicates the DHCP lease expiration time of the IPv6 subnet. The value can be -1, which indicates unlimited

Parameter	Mandator y	Type	Description
			lease time, or <i>Numberh</i> . The number ranges from 1 to 175200 . For example, the value can be 5h . The default value is 2h .
opt_name	Yes	String	- Specifies the NTP server address or DHCP lease expiration time configured for the subnet. - Currently, the value can be ntp, domainname, addresstime, or ipv6_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"
      },
      {
        "opt_value": "24h",
        "opt_name": "addresstime"
      }
    ],
    "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, 11th to 2,000th resource records will be returned. The default value of limit is 2000.
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 that the subnet belongs to. The value of this parameter is the AZ specified when the subnet is created and does not limit the usage scope of the subnet.
vpc_id	String	Specifies the ID of the VPC that the subnet belongs to.
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. <i>{publicBorderGroup}</i>: The subnet is used in a public border group. The public border group limits the usage scope of a subnet but can have multiple edge AZs associated. You can obtain the AZs by the API for Listing AZs.
tenant_id	String	Project ID

Parameter	Type	Description
created_at	String	- Specifies the time (UTC) when the subnet is created. - Format: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	- Specifies the time (UTC) when the subnet is updated. - Format: <i>yyyy-MM-ddTHH:mm:ss</i>

Table 4-37 extra_dhcp_opt object

Parameter	Mandatory	Type	Description
opt_value	No	String	- Specifies the NTP server address domain name, or DHCP lease expiration time configured for the subnet. - Constraints: - If opt_name is set to ntp, the value 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 (.). If opt_name is set to null, the value indicates that no NTP server is configured for the subnet. The parameter value cannot be an empty string. - If opt_name is set to domainname, the value is the domain name configured for DNS and is used to obtain the IP address from the DNS server. A domain name can contain only letters, digits, and hyphens (-) and cannot start or end with a hyphen (-). Each domain name contains at least two labels separated by periods (.). Max total: 254 characters. Max label: 63 characters. - The option addresstime for opt_name indicates the DHCP lease expiration time of the IPv4 subnet. The value can be -1, which indicates unlimited lease time, or Numberh. The number ranges from 1 to 175200. For example, the value can be 5h. The default value is 87600h. - The option ipv6_addresstime for opt_name indicates the DHCP lease expiration time of the IPv6 subnet. The value can be -1, which indicates unlimited

Parameter	Mandatory	Type	Description
			lease time, or <i>Numberh</i> . The number ranges from 1 to 175200 . For example, the value can be 5h . The default value is 2h .
opt_name	Yes	String	- Specifies the NTP server address or DHCP lease expiration time configured for the subnet. - Currently, the value can be ntp, domainname, addresstime, or ipv6_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"
        },
        {
          "opt_value": "24h",
          "opt_name": "addresstime"
        },
        {
          "opt_value": "2h",
          "opt_name": "ipv6_addresstime"
        }
      ],
      "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"
    },
    {
      "opt_value": "24h",
      "opt_name": "addressstime"
    }
  ],
  "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 >).

Parameter	Mandatory	Type	Description
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_opts 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 domain name, or DHCP lease expiration time configured for the subnet. - Constraints: - If opt_name is set to ntp, the value 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 (.). If opt_name is set to null, the value indicates that no NTP server is configured for the subnet. The parameter value cannot be an empty string. - If opt_name is set to domainname, the value is the domain name configured for DNS and is used to obtain the IP address from the DNS server. A domain name can contain only letters, digits, and hyphens (-) and cannot start or end with a hyphen (-). Each domain name contains at least two labels separated by periods (.). Max total: 254 characters. Max label: 63 characters. - The option addresstime for opt_name indicates the DHCP lease expiration time of the IPv4 subnet. The value can be -1, which indicates unlimited lease time, or Numberh. The number ranges from 1 to 175200. For example, the value can be 5h. The default value is 87600h. - The option ipv6_addresstime for opt_name indicates the DHCP lease expiration time of the IPv6 subnet. The value can be -1, which indicates unlimited

Parameter	Mandator y	Type	Description
			lease time, or <i>Numberh</i> . The number ranges from 1 to 175200 . For example, the value can be 5h . The default value is 2h .
opt_name	Yes	String	- Specifies the NTP server address or DHCP lease expiration time configured for the subnet. - Currently, the value can be ntp, domainname, addresstime, or ipv6_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"
      },
      {
        "opt_value": "24h",
        "opt_name": "addresstime"
      },
      {
        "opt_value": "2h",
        "opt_name": "ipv6_addresstime"
      }
    ]
  }
}
```

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, VPNs, and EIPs.

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 flow 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 flow 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 (<i>xxx</i> 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 (<i>xxx</i> 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	Mandator y	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, 11th to 2,000th resource records will be returned. The default value of limit is 2000.
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 value is mutually exclusive with parameters remote_group_id and remote_address_group_id.
remote_group_id	String	- Specifies the ID of the peer security group. - The parameter value is mutually exclusive with parameters remote_ip_prefix and remote_address_group_id.
remote_address_group_id	String	- Specifies the remote IP address group ID. - The parameter 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 value is mutually exclusive with parameters remote_group_id and remote_address_group_id.
remote_group_id	String	- Specifies the ID of the peer security group. - The parameter value is mutually exclusive with parameters remote_ip_prefix and remote_address_group_id.
remote_address_group_id	String	- Specifies the remote IP address group ID. - The parameter 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, 11th to 2,000th resource records will be returned. The default value of limit is 2000.

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 parameter 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 value is mutually exclusive with parameters remote_group_id and remote_address_group_id.
remote_group_id	String	- Specifies the ID of the peer security group. - The parameter value is mutually exclusive with parameters remote_ip_prefix and remote_address_group_id.
remote_address_group_id	String	- Specifies the remote IP address group ID. - The parameter 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 Adding a Security Group Rule

Function

This API is used to add 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. - Constraints: The parameter is mutually exclusive with remote_group_id and remote_address_group_id.
remote_group_id	No	String	- Specifies the ID of the peer security group. - Constraints: The parameter is mutually exclusive with 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 parameter 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 value is mutually exclusive with parameters remote_group_id and remote_address_group_id.

Parameter	Type	Description
remote_group_id	String	- Specifies the ID of the peer security group. - The parameter value is mutually exclusive with parameters remote_ip_prefix and remote_address_group_id.
remote_address_group_id	String	- Specifies the remote IP address group ID. - The parameter 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 value is mutually exclusive with parameters remote_group_id and remote_address_group_id.
remote_group_id	String	- Specifies the ID of the peer security group. - The parameter value is mutually exclusive with parameters remote_ip_prefix and remote_address_group_id.
remote_address_group_id	String	- Specifies the remote IP address group ID. - The parameter 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, 11th to 2,000th resource records will be returned. The default value of limit is 2000.

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.
remote_ip_prefix	No	String	Specifies the remote IP address. The value must be in CIDR format.

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.

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 value is mutually exclusive with parameters remote_group_id and remote_address_group_id.
remote_group_id	String	- Specifies the ID of the peer security group. - The parameter value is mutually exclusive with parameters remote_ip_prefix and remote_address_group_id.
remote_address_group_id	String	- Specifies the remote IP address group ID. - The parameter 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 that carries private IP addresses of a subnet. The port can be allocated to other cloud service resources, such as an ECS or a virtual IP address.

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.

Parameter	Mandatory	Type	Description
network_id	Yes	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	No	Boolean	- Specifies the administrative state of the port. - The default value is true.
device_owner	No	String	- Definition: Specifies the device that the port belongs to, that is, a cloud service resource that uses a private IP address in the subnet. - Range: 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.

Parameter	Mandatory	Type	Description
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.
allowed_address_pairs	No	Array of allowed_address_pairs 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 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 network interface 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 network interface 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 of the IPv4 network interface. If the value of this parameter is set to 651 , indicating the DHCP lease time of the IPv6 network interface.
opt_value	No	String	- Specifies the value of the DHCP option. - If the value of opt_name is 51 or 651, the value format of opt_value is Xh, indicating that the DHCP lease time is <i>X</i> hours. - The value of <i>X</i> is -1 or from 1 to 175200. 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 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 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.

Parameter	Type	Description
device_id	String	Definition: Specifies the ID of the device that the port belongs to. The device ID indicates the ID of the cloud service resource that uses the private IP address in the subnet, for example, the cloud server ID or load balancer ID.
device_owner	String	- Definition: Specifies the device that the port belongs to, that is, a cloud service resource that uses a private IP address in the subnet. - Range: network:dhcp: DHCP service network:router_interface_distributed: Subnet gateway address compute:xxx: Private IP address of a cloud server network interface. <i>XXX</i> specifies the AZ name. For example, compute:aa-bb-cc indicates that the private IP address is used by a cloud server in the AZ aa-bb-cc. neutron:VIP_PORT: Virtual IP address neutron:LOADBALANCERV2: Shared load balancer neutron:LOADBALANCERV3: Dedicated load balancer network:endpoint_interface: VPC endpoint network:nat_gateway: NAT gateway network:ucmp: UCMP port, which is used by Enterprise Router.
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.

Parameter	Type	Description
security_groups	Array of strings	Specifies the security group UUID (extended attribute).
allowed_address_pairs	Array of allowed_address_pairs 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 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 network interface 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: <code>{"internal_elb": true}</code> - 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: <code>{"disable_security_groups": true }</code> 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 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 network interface. - This parameter is displayed only when the IPv6 network interface 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 network interface 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 of the IPv4 network interface. If the value of this parameter is set to 651 , indicating the DHCP lease time of the IPv6 network interface.

Parameter	Type	Description
opt_value	String	- Specifies the value of the DHCP option. - If the value of opt_name is 51 or 651, the value format of opt_value is <i>Xh</i>, indicating that the DHCP lease time is <i>X</i> hours. - The value of <i>X</i> is -1 or from 1 to 175200. 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_efa": 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. A port is used to carry private IP addresses in a subnet.

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.

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 4-102. - 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	Definition: Specifies the ID of the device that the port belongs to. The device ID indicates the ID of the cloud service resource that uses the private IP address in the subnet, for example, the cloud server ID or load balancer ID.
device_owner	String	- Definition: Specifies the device that the port belongs to, that is, a cloud service resource that uses a private IP address in the subnet. - Range: network:dhcp: DHCP service network:router_interface_distributed: Subnet gateway address compute:xxx: Private IP address of a cloud server network interface. <i>XXX</i> specifies the AZ name. For example, compute:aa-bb-cc indicates that the private IP address is used by a cloud server in the AZ aa-bb-cc. neutron:VIP_PORT: Virtual IP address neutron:LOADBALANCERV2: Shared load balancer neutron:LOADBALANCERV3: Dedicated load balancer network:endpoint_interface: VPC endpoint network:nat_gateway: NAT gateway network:ucmp: UCMP port, which is used by Enterprise Router.
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. 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).
allowed_address_pairs	Array of allowed_address_pairs 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 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 network interface to 1.1.1.1/0.
extra_dhcp_opts	Array of extra_dhcp_option 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: <code>{"internal_elb": true}</code> • 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: <code>{"disable_security_groups": true }</code> 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 network interface. - This parameter is displayed only when the IPv6 network interface 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 network interface 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 of the IPv4 network interface. If the value of this parameter is set to 651 , indicating the DHCP lease time of the IPv6 network interface.

Parameter	Type	Description
opt_value	String	- Specifies the value of the DHCP option. - If the value of opt_name is 51 or 651, the value format of opt_value is Xh, indicating that the DHCP lease time is <i>X</i> hours. - The value of <i>X</i> is -1 or from 1 to 175200. 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_efa": false
}
```

Status Code

See [Status Codes](#).

Error Code

See [Error Codes](#).

4.6.3 Querying Ports

Function

This API is used to query multiple ports. The ports are used to carry private IP addresses in a subnet.

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_ad
dress={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	Mandat ory	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.

Parameter	Mandatory	Type	Description
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.
mac_address	No	String	Specifies the MAC address that is used as the filter.
device_id	No	String	Definition: Specifies the device ID that is used as the filter. The port belongs to the device with the ID. The device ID indicates the ID of the cloud service resource that uses the private IP address in the subnet, for example, the cloud server ID or load balancer ID.
device_owner	No	String	- Definition: Specifies the device owner that is used as the filter. The port belongs to the device, that is, a cloud service resource that uses a private IP address in the subnet. - For details about value range, see parameter device_owner in Table 4-109.
status	No	String	- Specifies the status of the port that is used as the filter. - The value can be ACTIVE, BUILD, or DOWN.

Parameter	Mandatory	Type	Description
security_groups	No	Array of strings	Specifies the UUID of the security group that is used as the filter.
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, 11th to 2,000th resource records will be returned. The default value of limit is 2000.

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.
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 <i>{ip_address}</i> to an IP address, for example, 192.168.21.22. Set <i>{subnet_id}</i> to an IPv4 or IPv6 subnet ID, for example, 011fc878-5521-4654-a1ad-f5b0b5820302.

Parameter	Mandatory	Type	Description
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.
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	Definition: Specifies the ID of the device that the port belongs to. The device ID indicates the ID of the cloud service resource that uses the private IP address in the subnet, for example, the cloud server ID or load balancer ID.

Parameter	Type	Description
device_owner	String	• Definition: Specifies the device that the port belongs to, that is, a cloud service resource that uses a private IP address in the subnet. • Range: – network:dhcp: DHCP service – network:router_interface_distributed: Subnet gateway address – compute:xxx: Private IP address of a cloud server network interface. <i>XXX</i> specifies the AZ name. For example, compute:aa-bb-cc indicates that the private IP address is used by a cloud server in the AZ aa-bb-cc. – neutron:VIP_PORT: Virtual IP address – neutron:LOADBALANCERV2: Shared load balancer – neutron:LOADBALANCERV3: Dedicated load balancer – network:endpoint_interface: VPC endpoint – network:nat_gateway: NAT gateway – network:ucmp: UCMP port, which is used by Enterprise Router.
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 a set of zero or more allowed address pairs. An address pair consists of an IP address and 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 network interface 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_option 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: <code>{"internal_elb": true}</code> • 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: <code>{"disable_security_groups": true }</code> 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 network interface. - This parameter is displayed only when the IPv6 network interface 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 network interface 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 of the IPv4 network interface. If the value of this parameter is set to 651 , indicating the DHCP lease time of the IPv6 network interface.

Parameter	Type	Description
opt_value	String	- Specifies the value of the DHCP option. - If the value of opt_name is 51 or 651, the value format of opt_value is <i>Xh</i>, indicating that the DHCP lease time is <i>X</i> hours. - The value of <i>X</i> is -1 or from 1 to 175200. 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_efa": 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_efa": 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. For example, you can update the security group of the cloud service resource that the port belongs to and associate the port with an ECS or virtual IP address.

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. For example, if this API is used to change the security group of an ECS, port_id is the ID of the ECS network interface.
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.

Parameter	Mandatory	Type	Description
security_groups	No	Array of strings	- Specifies the UUID of the security group. This is an extended attribute. - This parameter cannot be left blank.
allowed_address_pairs	No	Array of allowed_address_pairs 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 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 network interface 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 network interface 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 of the IPv4 network interface. If the value of this parameter is set to 651 , indicating the DHCP lease time of the IPv6 network interface.

Parameter	Mandatory	Type	Description
opt_value	No	String	- Specifies the value of the DHCP option. - If the value of opt_name is 51 or 651, the value format of opt_value is Xh, indicating that the DHCP lease time is <i>X</i> hours. - The value of <i>X</i> is -1 or from 1 to 175200. 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": "abc"
  }
}
```

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.

Parameter	Type	Description
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 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	Definition: Specifies the ID of the device that the port belongs to. The device ID indicates the ID of the cloud service resource that uses the private IP address in the subnet, for example, the cloud server ID or load balancer ID.

Parameter	Type	Description
device_owner	String	• Definition: Specifies the device that the port belongs to, that is, a cloud service resource that uses a private IP address in the subnet. • Range: – network:dhcp: DHCP service – network:router_interface_distributed: Subnet gateway address – compute:xxx: Private IP address of a cloud server network interface. <i>XXX</i> specifies the AZ name. For example, compute:aa-bb-cc indicates that the private IP address is used by a cloud server in the AZ aa-bb-cc. – neutron:VIP_PORT: Virtual IP address – neutron:LOADBALANCERV2: Shared load balancer – neutron:LOADBALANCERV3: Dedicated load balancer – network:endpoint_interface: VPC endpoint – network:nat_gateway: NAT gateway – network:ucmp: UCMP port, which is used by Enterprise Router.
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 a set of zero or more allowed address pairs. 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 network interface to 1.1.1.1/0.
extra_dhcp_opts	Array of extra_dhcp_option 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: <code>{"internal_elb": true}</code> • 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: <code>{"disable_security_groups": true }</code> 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 network interface. - This parameter is displayed only when the IPv6 network interface 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 network interface 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 of the IPv4 network interface. If the value of this parameter is set to 651 , indicating the DHCP lease time of the IPv6 network interface.

Parameter	Type	Description
opt_value	String	- Specifies the value of the DHCP option. - If the value of opt_name is 51 or 651, the value format of opt_value is Xh, indicating that the DHCP lease time is <i>X</i> hours. - The value of <i>X</i> is -1 or from 1 to 175200. 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": "abc",
    "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. A port is used to carry private IP addresses in a subnet.

Constraints

- If **device_owner** is not empty, the port cannot be deleted. However, there is a special case. If **device_owner** is **neutron:VIP_PORT**, the port can be deleted.
- If **device_id** is not empty, the port 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={mar  
ker}
```

[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.
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.

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, 11th to 2,000th resource records will be returned. The default value of limit is 2000.
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.
status	String	Specifies the status: • PENDING_ACCEPTANCE • REJECTED • EXPIRED • DELETED • ACTIVE
request_vpc_info	vpc_info object	Specifies information about the local VPC. For details, see Table 4-130 .

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

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	Mandato ry	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 status: • PENDING_ACCEPTANCE • REJECTED • EXPIRED • DELETED • ACTIVE
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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the VPC peering connection is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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.
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.

Attribute	Mandatory	Type	Description
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.

Attribute	Type	Description
status	String	Specifies the status: • 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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the VPC peering connection is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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	Mandato ry	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 status: • PENDING_ACCEPTANCE • REJECTED • EXPIRED • DELETED • ACTIVE
request_vpc_info	vpc_info object	Specifies information about the local VPC. For details, see Table 4-144 .
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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the VPC peering connection is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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	Mandato ry	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.
status	String	Specifies the status: 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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the VPC peering connection is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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 status: • 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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the VPC peering connection is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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}&marker={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.
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, 11th to 2,000th resource records will be returned. The default value of limit is 2000.
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, 11th to 2,000th resource records will be returned. The default value of limit is 2000.

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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	- Specifies the time (UTC) when the route table is updated. - Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	- Specifies the time (UTC) when the route table is updated. - Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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. 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 is 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 up to 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. 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 is 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 **routeable-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": "routeable-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	routeable 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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	- Specifies the time (UTC) when the route table is updated. - Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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. 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 is 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. 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. 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 is 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. 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 is 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": "routetable-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 **route** 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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	- Specifies the time (UTC) when the route table is updated. - Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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. 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 is 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}/v1/6fbc9263116a4b68818cf1edce16bc4f/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 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 4-201. - 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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	- Specifies the time (UTC) when the route table is updated. - Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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. 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 is 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 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 4-209. - 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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	- Specifies the time (UTC) when the route table is updated. - Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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. 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. - Can contain a maximum of 128 characters. - Can contain letters, digits, underscores (_), and hyphens (-). - The tag key of a VPC must be unique.
value	String	Yes	- Specifies the tag value. - Can contain a maximum of 255 characters. - 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. - Can contain a maximum of 128 characters. - Can contain letters, digits, underscores (_), and hyphens (-). - The tag key of a VPC must be unique.
value	String	- Specifies the tag value. - Can contain a maximum of 255 characters. - 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. • Can contain a maximum of 128 characters. • Can contain letters, digits, underscores (_), and hyphens (-). • The tag key of a VPC must be unique.
value	String	Yes	• Specifies the tag value. • Can contain a maximum of 255 characters. • 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. - Can contain a maximum of 128 characters. - Can contain letters, digits, underscores (_), and hyphens (-). - The tag key of a VPC must be unique.
value	String	Yes	- Specifies the tag value. - Can contain a maximum of 255 characters. - 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. - Can contain a maximum of 128 characters. - Can contain letters, digits, underscores (_), and hyphens (-). - The tag key of a VPC must be unique.
value	String	- Specifies the tag value. - Can contain a maximum of 255 characters. - 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 a 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. - Can contain a maximum of 128 characters. - Can contain letters, digits, underscores (_), and hyphens (-). - The tag key of a VPC must be unique.
value	String	Yes	- Specifies the tag value. - Can contain a maximum of 255 characters. - 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": "cdfc_cdfs_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 Are the Differences 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

Flow logs are available only in certain regions. For details, visit [Function Overview](#) and click **Flow Log**.

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	Specifies the 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 up to 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: a single network interface. vpc: All network interfaces in a VPC. network: All network interfaces 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 up to 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 >).

Parameter	Type	Description
resource_type	String	- Type of the resource for which that the logs to be collected. - The value can be: port: a single network interface. vpc: All network interfaces in a VPC. network: All network interfaces 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
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:mm:ss
updated_at	String	- Time when the flow log is updated - UTC time in the format of yyyy-MM-ddTHH:mm:ss

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	Mandato ry	Type	Description
project_id	Yes	String	Project ID. For details, see Obtaining a Project ID.

Parameter	Mandatory	Type	Description
id	No	String	Flow log ID
name	No	String	- Flow log name - The value can contain up to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
tenant_id	No	String	Project ID
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: a single network interface. vpc: All network interfaces in a VPC. network: All network interfaces in a subnet.
resource_id	No	String	ID of the resource for which that the logs to be collected.

Parameter	Mandatory	Type	Description
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
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, 11th to 2,000th resource records will be returned. The default value of limit is 2000.

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 up to 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: a single network interface. vpc: All network interfaces in a VPC. network: All network interfaces 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:mm:ss
updated_at	String	- Time when the flow log is updated - UTC time in the format of yyyy-MM-ddTHH:mm:ss

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, 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 up to 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: a single network interface. vpc: All network interfaces in a VPC. network: All network interfaces 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:mm:ss
updated_at	String	- Time when the flow log is updated - UTC time in the format of yyyy-MM-ddTHH:mm:ss

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, 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 up to 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

Parameter	Type	Description
name	String	- Flow log name - The value can contain up to 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: a single network interface. vpc: All network interfaces in a VPC. network: All network interfaces 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:mm:ss
updated_at	String	- Time when the flow log is updated - UTC time in the format of yyyy-MM-ddTHH:mm:ss

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, 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 VPC APIs (V3)

5.1 VPC

5.1.1 Querying VPCs

Function

After a VPC is created, you can call this API to query all information about the VPC, including the VPC name, ID, and CIDR block.

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.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v3/{project_id}/vpc/vpcs

Table 5-1 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	- Definition: ID of the project that a VPC belongs to. For details about how to obtain a project ID, see Obtaining a Project ID. - Range: None

Table 5-2 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	- Definition: Number of records returned on each page. - Range: 0-2000
marker	No	String	- Definition: ID of the resource from which the pagination query starts. If the parameter is left blank, only resources on the first page are queried. - Range: VPC ID.
id	No	Array of strings	- Definition: VPC ID, which can be used to filter VPCs. - Range: None
name	No	Array of strings	- Definition: VPC name, which can be used to filter VPCs. - Range: None
description	No	Array of strings	- Definition: VPC description, which can be used to filter VPCs. - Range: None
cidr	No	Array of strings	- Definition: CIDR block of a VPC, which can be used to filter VPCs. - Range: None

Request Parameters

None

Response Parameters

Status code: 200

Table 5-3 Response body parameters

Parameter	Type	Description
request_id	String	- Definition: Request ID. - Range: None

Parameter	Type	Description
vpcs	Array of Vpc objects	- Definition: Response body for querying VPCs. - Range: None
page_info	PageInfo object	- Definition: Pagination information. - Range: None

Table 5-4 Vpc

Parameter	Type	Description
id	String	- Definition: VPC ID. After a VPC is created, a VPC ID is generated, which uniquely identifies the VPC. - Range: The value is in UUID format with hyphens (-).
name	String	- Definition: VPC name. - Range: The value can contain 0 to 64 characters. It can include letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	- Definition: Description of a VPC. - Range: The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
cidr	String	- Definition: Available subnets in a VPC. - Range: 10.0.0.0/8–24: The IP address ranges from 10.0.0.0 to 10.255.255.255, and the netmask ranges from 8 to 24. 172.16.0.0/12–24: The IP address ranges from 172.16.0.0 to 172.31.255.255, and the netmask ranges from 12 to 24. 192.168.0.0/16–24: The IP address ranges from 192.168.0.0 to 192.168.255.255, and the netmask ranges from 16 to 24. - If cidr is not specified, the default value is "".

Parameter	Type	Description
extend_cidrs	Array of strings	• Definition: Secondary CIDR blocks of a VPC. • Range: The following CIDR blocks are not supported: – 10.0.0.0/8: The IP address range is 10.0.0.0-10.255.255.255. – 172.16.0.0/12: The IP address range is 172.16.0.0-172.31.255.255. – 192.168.0.0/16: The IP address range is 192.168.0.0-192.168.255.255. – 172.31.0.0/16: The IP address range is 172.31.0.0-172.31.255.255. – 100.64.0.0/10: The IP address range is 100.64.0.0-100.127.255.255. – 214.0.0.0/7: The IP address range is 214.0.0.0-215.255.255.255. – 198.18.0.0/15: The IP address range is 198.18.0.0-198.19.255.255. – 169.254.0.0/16: The IP address range is 169.254.0.0-169.254.255.255. – 0.0.0.0/8: The IP address range is 0.0.0.0-0.255.255.255. – 127.0.0.0/8: The IP address range is 127.0.0.0-127.255.255.255. – 240.0.0.0/4: The IP address range is 240.0.0.0-255.255.255.255.
status	String	• Definition: VPC status. • Range: – PENDING: The VPC is being created. – ACTIVE: The VPC is created.
project_id	String	• Definition: ID of the project that a VPC belongs to. • Range: None

Parameter	Type	Description
enterprise_project_id	String	- Definition: ID of the enterprise project that a VPC belongs to. - Range: The value is 0 or a string that contains a maximum of 36 characters in UUID format with hyphens (-). 0 indicates the default enterprise project.
created_at	String	- Definition: Time when a VPC was created. - Range: UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
updated_at	String	- Definition: Time when a VPC was updated. - Range: UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
cloud_resources	Array of CloudResource objects	- Definition: Type and number of resources associated with a VPC. For example, subnets and route tables. - Range: None
tags	Array of ResponseTag objects	- Definition: Tags of a VPC, including tag keys and tag values, which can be used to classify and identify resources. For details, see the tag objects. - Range: None

Table 5-5 CloudResource

Parameter	Type	Description
resource_type	String	- Definition: Resource type. - Range: None
resource_count	Integer	- Definition: Number of resources. - Range: None

Table 5-6 ResponseTag

Parameter	Type	Description
key	String	Definition: Tag key. Range: • A tag key can contain a maximum of 128 Unicode characters and cannot be left blank. • Each tag key of a resource must be unique. • The value can contain: – Letters – Digits – Special characters: underscores (_), hyphens (-) – Chinese characters
value	String	Definition: Tag value. Range: • Each value can contain a maximum of 255 Unicode characters and can be left blank. • The value can contain: – Letters – Digits – Special characters: underscores (_), hyphens (-), periods (.) – Chinese characters

Table 5-7 PageInfo

Parameter	Type	Description
previous_marker	String	Definition: The first record on the current page. Range: N/A

Parameter	Type	Description
current_count	Integer	Definition: Total number of resources on the current page. Range: N/A
next_marker	String	Definition: The last record on the current page. The next_marker field does not exist if the page is the last one. Range: N/A

Example Requests

- 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
```

Example Responses

Status code: 200

Normal response to the GET operation. For more status codes, see [Status Code](#).

```
{  
  "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
}
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class ListVpcsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
```

```
environment variables and decrypted during use to ensure security.
// In this example, AK and SK are stored in environment variables for authentication. Before running
this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
String ak = System.getenv("CLOUD_SDK_AK");
String sk = System.getenv("CLOUD_SDK_SK");
String projectId = "{project_id}";

ICredential auth = new BasicCredentials()
    .withProjectId(projectId)
    .withAk(ak)
    .withSk(sk);

VpcClient client = VpcClient.newBuilder()
    .withCredential(auth)
    .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
    .build();
ListVpcsRequest request = new ListVpcsRequest();
try {
    ListVpcsResponse response = client.listVpcs(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListVpcsRequest()
        response = client.list_vpcs(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
```

```
print(e.error_code)
print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListVpcsRequest{}
    response, err := client.ListVpcs(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Normal response to the GET operation. For more status codes, see Status Code .

Error Codes

See [Error Codes](#).

5.1.2 Querying the Details of a VPC

Function

After a VPC is created, you can call this API to query all information about the VPC, including the VPC name, ID, and CIDR block.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v3/{project_id}/vpc/vpcs/{vpc_id}

Table 5-8 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	- Definition: ID of the project that a VPC belongs to. For details about how to obtain a project ID, see Obtaining a Project ID. - Range: None
vpc_id	Yes	String	- Definition: VPC ID, which uniquely identifies the VPC. - Range: None

Request Parameters

None

Response Parameters

Status code: 200

Table 5-9 Response body parameters

Parameter	Type	Description
request_id	String	- Definition: Request ID. - Range: None
vpc	Vpc object	- Definition: Response body for querying details about a VPC. - Range: None

Table 5-10 Vpc

Parameter	Type	Description
id	String	- Definition: VPC ID. After a VPC is created, a VPC ID is generated, which uniquely identifies the VPC. - Range: The value is in UUID format with hyphens (-).
name	String	- Definition: VPC name. - Range: The value can contain 0 to 64 characters. It can include letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	- Definition: Description of a VPC. - Range: The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
cidr	String	- Definition: Available subnets in a VPC. - Range: 10.0.0.0/8-24: The IP address ranges from 10.0.0.0 to 10.255.255.255, and the netmask ranges from 8 to 24. 172.16.0.0/12-24: The IP address ranges from 172.16.0.0 to 172.31.255.255, and the netmask ranges from 12 to 24. 192.168.0.0/16-24: The IP address ranges from 192.168.0.0 to 192.168.255.255, and the netmask ranges from 16 to 24. - If cidr is not specified, the default value is "".

Parameter	Type	Description
extend_cidrs	Array of strings	• Definition: Secondary CIDR blocks of a VPC. • Range: The following CIDR blocks are not supported: – 10.0.0.0/8: The IP address range is 10.0.0.0-10.255.255.255. – 172.16.0.0/12: The IP address range is 172.16.0.0-172.31.255.255. – 192.168.0.0/16: The IP address range is 192.168.0.0-192.168.255.255. – 172.31.0.0/16: The IP address range is 172.31.0.0-172.31.255.255. – 100.64.0.0/10: The IP address range is 100.64.0.0-100.127.255.255. – 214.0.0.0/7: The IP address range is 214.0.0.0-215.255.255.255. – 198.18.0.0/15: The IP address range is 198.18.0.0-198.19.255.255. – 169.254.0.0/16: The IP address range is 169.254.0.0-169.254.255.255. – 0.0.0.0/8: The IP address range is 0.0.0.0-0.255.255.255. – 127.0.0.0/8: The IP address range is 127.0.0.0-127.255.255.255. – 240.0.0.0/4: The IP address range is 240.0.0.0-255.255.255.255.
status	String	• Definition: VPC status. • Range: – PENDING: The VPC is being created. – ACTIVE: The VPC is created.
project_id	String	• Definition: ID of the project that a VPC belongs to. • Range: None

Parameter	Type	Description
enterprise_project_id	String	- Definition: ID of the enterprise project that a VPC belongs to. - Range: The value is 0 or a string that contains a maximum of 36 characters in UUID format with hyphens (-). 0 indicates the default enterprise project.
created_at	String	- Definition: Time when a VPC was created. - Range: UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
updated_at	String	- Definition: Time when a VPC was updated. - Range: UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
cloud_resources	Array of CloudResource objects	- Definition: Type and number of resources associated with a VPC. For example, subnets and route tables. - Range: None
tags	Array of ResponseTag objects	- Definition: Tags of a VPC, including tag keys and tag values, which can be used to classify and identify resources. For details, see the tag objects. - Range: None

Table 5-11 CloudResource

Parameter	Type	Description
resource_type	String	- Definition: Resource type. - Range: None
resource_count	Integer	- Definition: Number of resources. - Range: None

Table 5-12 ResponseTag

Parameter	Type	Description
key	String	Definition: Tag key. Range: • A tag key can contain a maximum of 128 Unicode characters and cannot be left blank. • Each tag key of a resource must be unique. • The value can contain: – Letters – Digits – Special characters: underscores (_), hyphens (-) – Chinese characters
value	String	Definition: Tag value. Range: • Each value can contain a maximum of 255 Unicode characters and can be left blank. • The value can contain: – Letters – Digits – Special characters: underscores (_), hyphens (-), periods (.) – Chinese characters

Example Requests

Querying the details of a VPC

```
GET https://{Endpoint}/v3/{project_id}/vpc/vpcs/0552091e-b83a-49dd-88a7-4a5c86fd9ec3
```

Example Responses

Status code: 200

Normal response to the GET operation. For more status codes, see [Status Code](#).

```
{
  "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" : "2018-03-23T09:26:08",
"updated_at" : "2018-08-24T08:49:53"
}
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class ShowVpcSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();
        ShowVpcRequest request = new ShowVpcRequest();
        request.withVpcId("{vpc_id}");
        try {
            ShowVpcResponse response = client.showVpc(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
        }
    }
}
```

```
        e.printStackTrace();
        System.out.println(e.getHttpStatusCode());
        System.out.println(e.getRequestId());
        System.out.println(e.getErrorCode());
        System.out.println(e.getErrorMsg());
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowVpcRequest()
        request.vpc_id = "{vpc_id}"
        response = client.show_vpc(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"
```

```
auth := basic.NewCredentialsBuilder().
    WithAk(ak).
    WithSk(sk).
    WithProjectId(projectId).
    Build()

client := vpc.NewVpcClient(
    vpc.VpcClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.ShowVpcRequest{}
request.VpcId = "{vpc_id}"
response, err := client.ShowVpc(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Normal response to the GET operation. For more status codes, see Status Code .

Error Codes

See [Error Codes](#).

5.1.3 Adding a Secondary CIDR Block to a VPC

Function

The IPv4 CIDR block you specify when you create a VPC is the primary one. The primary CIDR block cannot be changed after the VPC is created. If IP addresses in the primary CIDR block are insufficient, you can call this API to add a secondary CIDR block to a VPC.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v3/{project_id}/vpc/vpcs/{vpc_id}/add-extend-cidr

Table 5-13 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	- Definition: ID of the project that a VPC belongs to. For details about how to obtain a project ID, see Obtaining a Project ID. - Range: None
vpc_id	Yes	String	- Definition: VPC ID, which uniquely identifies the VPC. - Range: None

Request Parameters

Table 5-14 Request body parameters

Parameter	Mandatory	Type	Description
dry_run	No	Boolean	- Definition: Whether to only send the check request. - Constraints: None - Range: true: Only the check request will be sent and no secondary CIDR block will not be added. Check items include mandatory parameters, request format, and constraints. If the check fails, an error will be returned. If the check succeeds, response code 202 will be returned. false: A request will be sent and a secondary CIDR block will be added. - Default Value: false

Parameter	Mandatory	Type	Description
vpc	Yes	AddExtendCidrOption object	• Definition: Request body for adding a secondary CIDR block. • Constraints: None • Range: None • Default Value: None

Table 5-15 AddExtendCidrOption

Parameter	Mandatory	Type	Description
extend_cidrs	Yes	Array of strings	• Definition: Secondary CIDR blocks of a VPC. • Constraints: Only IPv4 CIDR blocks are supported. • Range: The following CIDR blocks are not supported: – 10.0.0.0/8: The IP address range is 10.0.0.0-10.255.255.255. – 172.16.0.0/12: The IP address range is 172.16.0.0-172.31.255.255. – 192.168.0.0/16: The IP address range is 192.168.0.0-192.168.255.255. – 172.31.0.0/16: The IP address range is 172.31.0.0-172.31.255.255. – 100.64.0.0/10: The IP address range is 100.64.0.0-100.127.255.255. – 214.0.0.0/7: The IP address range is 214.0.0.0-215.255.255.255. – 198.18.0.0/15: The IP address range is 198.18.0.0-198.19.255.255. – 169.254.0.0/16: The IP address range is 169.254.0.0-169.254.255.255. – 0.0.0.0/8: The IP address range is 0.0.0.0-0.255.255.255. – 127.0.0.0/8: The IP address range is 127.0.0.0-127.255.255.255.

Parameter	Mandatory	Type	Description
			– 240.0.0.0/4: The IP address range is 240.0.0.0-255.255.255.255. • Default Value: None

Response Parameters

Status code: 200

Table 5-16 Response body parameters

Parameter	Type	Description
request_id	String	• Definition: Request ID. • Range: None
vpc	Vpc object	• Definition: Response body for adding a secondary CIDR block. • Range: None

Table 5-17 Vpc

Parameter	Type	Description
id	String	• Definition: VPC ID. After a VPC is created, a VPC ID is generated, which uniquely identifies the VPC. • Range: The value is in UUID format with hyphens (-).
name	String	• Definition: VPC name. • Range: The value can contain 0 to 64 characters. It can include letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	• Definition: Description of a VPC. • Range: The value can contain no more than 255 characters and cannot contain angle brackets (< or >).

Parameter	Type	Description
cidr	String	• Definition: Available subnets in a VPC. • Range: – 10.0.0.0/8–24: The IP address ranges from 10.0.0.0 to 10.255.255.255, and the netmask ranges from 8 to 24. – 172.16.0.0/12–24: The IP address ranges from 172.16.0.0 to 172.31.255.255, and the netmask ranges from 12 to 24. – 192.168.0.0/16–24: The IP address ranges from 192.168.0.0 to 192.168.255.255, and the netmask ranges from 16 to 24. – If cidr is not specified, the default value is "".

Parameter	Type	Description
extend_cidrs	Array of strings	• Definition: Secondary CIDR blocks of a VPC. • Range: The following CIDR blocks are not supported: – 10.0.0.0/8: The IP address range is 10.0.0.0-10.255.255.255. – 172.16.0.0/12: The IP address range is 172.16.0.0-172.31.255.255. – 192.168.0.0/16: The IP address range is 192.168.0.0-192.168.255.255. – 172.31.0.0/16: The IP address range is 172.31.0.0-172.31.255.255. – 100.64.0.0/10: The IP address range is 100.64.0.0-100.127.255.255. – 214.0.0.0/7: The IP address range is 214.0.0.0-215.255.255.255. – 198.18.0.0/15: The IP address range is 198.18.0.0-198.19.255.255. – 169.254.0.0/16: The IP address range is 169.254.0.0-169.254.255.255. – 0.0.0.0/8: The IP address range is 0.0.0.0-0.255.255.255. – 127.0.0.0/8: The IP address range is 127.0.0.0-127.255.255.255. – 240.0.0.0/4: The IP address range is 240.0.0.0-255.255.255.255.
status	String	• Definition: VPC status. • Range: – PENDING: The VPC is being created. – ACTIVE: The VPC is created.
project_id	String	• Definition: ID of the project that a VPC belongs to. • Range: None

Parameter	Type	Description
enterprise_project_id	String	- Definition: ID of the enterprise project that a VPC belongs to. - Range: The value is 0 or a string that contains a maximum of 36 characters in UUID format with hyphens (-). 0 indicates the default enterprise project.
created_at	String	- Definition: Time when a VPC was created. - Range: UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
updated_at	String	- Definition: Time when a VPC was updated. - Range: UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
cloud_resources	Array of CloudResource objects	- Definition: Type and number of resources associated with a VPC. For example, subnets and route tables. - Range: None
tags	Array of ResponseTag objects	- Definition: Tags of a VPC, including tag keys and tag values, which can be used to classify and identify resources. For details, see the tag objects. - Range: None

Table 5-18 CloudResource

Parameter	Type	Description
resource_type	String	- Definition: Resource type. - Range: None
resource_count	Integer	- Definition: Number of resources. - Range: None

Table 5-19 ResponseTag

Parameter	Type	Description
key	String	Definition: Tag key. Range: • A tag key can contain a maximum of 128 Unicode characters and cannot be left blank. • Each tag key of a resource must be unique. • The value can contain: – Letters – Digits – Special characters: underscores (_), hyphens (-) – Chinese characters
value	String	Definition: Tag value. Range: • Each value can contain a maximum of 255 Unicode characters and can be left blank. • The value can contain: – Letters – Digits – Special characters: underscores (_), hyphens (-), periods (.) – Chinese characters

Status code: 202

Table 5-20 Response body parameters

Parameter	Type	Description
request_id	String	• Definition: Request ID. • Range: None
error_msg	String	• Definition: Error message. • Range: None
error_code	String	• Definition: Error code. • Range: None

Example Requests

Add the secondary CIDR block 23.8.0.0/16 to the VPC whose ID is 0552091e-b83a-49dd-88a7-4a5c86fd9ec3.

```
PUT https://{Endpoint}/v3/{project_id}/vpc/vpcs/0552091e-b83a-49dd-88a7-4a5c86fd9ec3/add-extend-cidr
{
  "vpc": {
    "extend_cidrs": [ "23.8.0.0/16" ]
  }
}
```

Example Responses

Status code: 200

Normal response to the PUT operation. For more status codes, see [Status Code](#).

```
{
  "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": "2018-03-23T09:26:08",
    "updated_at": "2018-08-24T08:49:53"
  }
}
```

Status code: 202

Normal response to the specified preflight request of API V3. For more status codes, see [Status Code](#).

```
{
  "error_msg": "Request validation has been passed with dry run...",
  "error_code": "SYS.0202",
  "request_id": "cfd81aea3f59eac7128dba4b36d516c8"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Add the secondary CIDR block 23.8.0.0/16 to the VPC whose ID is 0552091e-b83a-49dd-88a7-4a5c86fd9ec3.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

import java.util.List;
import java.util.ArrayList;

public class AddVpcExtendCidrSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();
        AddVpcExtendCidrRequest request = new AddVpcExtendCidrRequest();
        request.withVpcId("{vpc_id}");
        AddVpcExtendCidrRequestBody body = new AddVpcExtendCidrRequestBody();
        List<String> listVpcExtendCidrs = new ArrayList<>();
        listVpcExtendCidrs.add("23.8.0.0/16");
        AddExtendCidrOption vpcbody = new AddExtendCidrOption();
        vpcbody.withExtendCidrs(listVpcExtendCidrs);
        body.withVpc(vpcbody);
        request.withBody(body);
        try {
            AddVpcExtendCidrResponse response = client.addVpcExtendCidr(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Add the secondary CIDR block 23.8.0.0/16 to the VPC whose ID is 0552091e-b83a-49dd-88a7-4a5c86fd9ec3.

```
# coding: utf-8

import os
```



```
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = AddVpcExtendCidrRequest()
        request.vpc_id = "{vpc_id}"
        listExtendCidrsVpc = [
            "23.8.0.0/16"
        ]
        vpcbody = AddExtendCidrOption(
            extend_cidrs=listExtendCidrsVpc
        )
        request.body = AddVpcExtendCidrRequestBody(
            vpc=vpcbody
        )
        response = client.add_vpc_extend_cidr(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Add the secondary CIDR block 23.8.0.0/16 to the VPC whose ID is 0552091e-b83a-49dd-88a7-4a5c86fd9ec3.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
```

```
WithSk(sk).
WithProjectId(projectId).
Build()

client := vpc.NewVpcClient(
    vpc.VpcClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.AddVpcExtendCidrRequest{}
request.VpcId = "{vpc_id}"
var listExtendCidrsVpc = []string{
    "23.8.0.0/16",
}
vpcbody := &model.AddExtendCidrOption{
    ExtendCidrs: listExtendCidrsVpc,
}
request.Body = &model.AddVpcExtendCidrRequestBody{
    Vpc: vpcbody,
}
response, err := client.AddVpcExtendCidr(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Normal response to the PUT operation. For more status codes, see Status Code .
202	Normal response to the specified preflight request of API V3. For more status codes, see Status Code .

Error Codes

See [Error Codes](#).

5.1.4 Removing a Secondary CIDR Block from a VPC

Function

If a secondary CIDR block of your VPC is no longer used, you can call this API to remove it from the VPC.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v3/{project_id}/vpc/vpcs/{vpc_id}/remove-extend-cidr

Table 5-21 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	- Definition: ID of the project that a VPC belongs to. For details about how to obtain a project ID, see Obtaining a Project ID. - Range: None
vpc_id	Yes	String	- Definition: VPC ID, which uniquely identifies the VPC. - Range: None

Request Parameters

Table 5-22 Request body parameters

Parameter	Mandatory	Type	Description
dry_run	No	Boolean	• Definition: Whether to only send the check request. • Constraints: None • Range: – true: Only the check request will be sent and no secondary CIDR block will be removed. Check items include mandatory parameters, request format, and constraints. If the check fails, an error will be returned. If the check succeeds, response code 202 will be returned. – false: A request will be sent and a secondary CIDR block will be removed. • Default Value: false
vpc	Yes	RemoveExtendedCidrOption object	• Definition: Request body for removing a secondary CIDR block from a VPC. • Constraints: None • Range: None • Default Value: None

Table 5-23 RemoveExtendCidrOption

Parameter	Mandatory	Type	Description
extend_cidrs	Yes	Array of strings	• Definition: Secondary CIDR block to be removed from a VPC. • Constraints: Before removing a secondary CIDR block, delete the subnets in the CIDR block first. • Range: The value must be the secondary CIDR blocks in the VPC. • Default Value: None

Response Parameters

Status code: 200

Table 5-24 Response body parameters

Parameter	Type	Description
request_id	String	• Definition: Request ID. • Range: None
vpc	Vpc object	• Definition: Response body for removing a secondary CIDR block from a VPC. • Range: None

Table 5-25 Vpc

Parameter	Type	Description
id	String	• Definition: VPC ID. After a VPC is created, a VPC ID is generated, which uniquely identifies the VPC. • Range: The value is in UUID format with hyphens (-).
name	String	• Definition: VPC name. • Range: The value can contain 0 to 64 characters. It can include letters, digits, underscores (_), hyphens (-), and periods (.).

Parameter	Type	Description
description	String	• Definition: Description of a VPC. • Range: The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
cidr	String	• Definition: Available subnets in a VPC. • Range: – 10.0.0.0/8–24: The IP address ranges from 10.0.0.0 to 10.255.255.255, and the netmask ranges from 8 to 24. – 172.16.0.0/12–24: The IP address ranges from 172.16.0.0 to 172.31.255.255, and the netmask ranges from 12 to 24. – 192.168.0.0/16–24: The IP address ranges from 192.168.0.0 to 192.168.255.255, and the netmask ranges from 16 to 24. – If cidr is not specified, the default value is "".

Parameter	Type	Description
extend_cidrs	Array of strings	• Definition: Secondary CIDR blocks of a VPC. • Range: The following CIDR blocks are not supported: – 10.0.0.0/8: The IP address range is 10.0.0.0-10.255.255.255. – 172.16.0.0/12: The IP address range is 172.16.0.0-172.31.255.255. – 192.168.0.0/16: The IP address range is 192.168.0.0-192.168.255.255. – 172.31.0.0/16: The IP address range is 172.31.0.0-172.31.255.255. – 100.64.0.0/10: The IP address range is 100.64.0.0-100.127.255.255. – 214.0.0.0/7: The IP address range is 214.0.0.0-215.255.255.255. – 198.18.0.0/15: The IP address range is 198.18.0.0-198.19.255.255. – 169.254.0.0/16: The IP address range is 169.254.0.0-169.254.255.255. – 0.0.0.0/8: The IP address range is 0.0.0.0-0.255.255.255. – 127.0.0.0/8: The IP address range is 127.0.0.0-127.255.255.255. – 240.0.0.0/4: The IP address range is 240.0.0.0-255.255.255.255.
status	String	• Definition: VPC status. • Range: – PENDING: The VPC is being created. – ACTIVE: The VPC is created.
project_id	String	• Definition: ID of the project that a VPC belongs to. • Range: None

Parameter	Type	Description
enterprise_project_id	String	- Definition: ID of the enterprise project that a VPC belongs to. - Range: The value is 0 or a string that contains a maximum of 36 characters in UUID format with hyphens (-). 0 indicates the default enterprise project.
created_at	String	- Definition: Time when a VPC was created. - Range: UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
updated_at	String	- Definition: Time when a VPC was updated. - Range: UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
cloud_resources	Array of CloudResource objects	- Definition: Type and number of resources associated with a VPC. For example, subnets and route tables. - Range: None
tags	Array of ResponseTag objects	- Definition: Tags of a VPC, including tag keys and tag values, which can be used to classify and identify resources. For details, see the tag objects. - Range: None

Table 5-26 CloudResource

Parameter	Type	Description
resource_type	String	- Definition: Resource type. - Range: None
resource_count	Integer	- Definition: Number of resources. - Range: None

Table 5-27 ResponseTag

Parameter	Type	Description
key	String	Definition: Tag key. Range: • A tag key can contain a maximum of 128 Unicode characters and cannot be left blank. • Each tag key of a resource must be unique. • The value can contain: – Letters – Digits – Special characters: underscores (_), hyphens (-) – Chinese characters
value	String	Definition: Tag value. Range: • Each value can contain a maximum of 255 Unicode characters and can be left blank. • The value can contain: – Letters – Digits – Special characters: underscores (_), hyphens (-), periods (.) – Chinese characters

Status code: 202**Table 5-28** Response body parameters

Parameter	Type	Description
request_id	String	• Definition: Request ID. • Range: None
error_msg	String	• Definition: Error message. • Range: None
error_code	String	• Definition: Error code. • Range: None

Example Requests

Remove the secondary CIDR block 23.8.0.0/16 from the VPC whose ID is 0552091e-b83a-49dd-88a7-4a5c86fd9ec3.

```
PUT https://{Endpoint}/v3/{project_id}/vpc/vpcs/0552091e-b83a-49dd-88a7-4a5c86fd9ec3/remove-extend-cidr

{
  "vpc": {
    "extend_cidrs": [ "23.8.0.0/16" ]
  }
}
```

Example Responses

Status code: 200

Normal response to the PUT operation. For more status codes, see [Status Code](#).

```
{
  "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": "2018-03-23T09:26:08",
    "updated_at": "2018-08-24T08:49:53"
  }
}
```

Status code: 202

Normal response to the specified preflight request of API V3. For more status codes, see [Status Code](#).

```
{
  "error_msg": "Request validation has been passed with dry run...",
  "error_code": "SYS.0202",
  "request_id": "cfd81aea3f59eac7128dba4b36d516c8"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Remove the secondary CIDR block 23.8.0.0/16 from the VPC whose ID is 0552091e-b83a-49dd-88a7-4a5c86fd9ec3.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

import java.util.List;
import java.util.ArrayList;

public class RemoveVpcExtendCidrSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();

        RemoveVpcExtendCidrRequest request = new RemoveVpcExtendCidrRequest();
        request.withVpcId("{vpc_id}");
        RemoveVpcExtendCidrRequestBody body = new RemoveVpcExtendCidrRequestBody();
        List<String> listVpcExtendCidrs = new ArrayList<>();
        listVpcExtendCidrs.add("23.8.0.0/16");
        RemoveExtendCidrOption vpcbody = new RemoveExtendCidrOption();
        vpcbody.withExtendCidrs(listVpcExtendCidrs);
        body.withVpc(vpcbody);
        request.withBody(body);
        try {
            RemoveVpcExtendCidrResponse response = client.removeVpcExtendCidr(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Remove the secondary CIDR block 23.8.0.0/16 from the VPC whose ID is 0552091e-b83a-49dd-88a7-4a5c86fd9ec3.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = RemoveVpcExtendCidrRequest()
        request.vpc_id = "{vpc_id}"
        listExtendCidrsVpc = [
            "23.8.0.0/16"
        ]
        vpcbody = RemoveExtendCidrOption(
            extend_cidrs=listExtendCidrsVpc
        )
        request.body = RemoveVpcExtendCidrRequestBody(
            vpc=vpcbody
        )
        response = client.remove_vpc_extend_cidr(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Remove the secondary CIDR block 23.8.0.0/16 from the VPC whose ID is 0552091e-b83a-49dd-88a7-4a5c86fd9ec3.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
```

```
variables and decrypted during use to ensure security.
// In this example, AK and SK are stored in environment variables for authentication. Before running this
example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak := os.Getenv("CLOUD_SDK_AK")
sk := os.Getenv("CLOUD_SDK_SK")
projectId := "{project_id}"

auth := basic.NewCredentialsBuilder().
    WithAk(ak).
    WithSk(sk).
    WithProjectId(projectId).
    Build()

client := vpc.NewVpcClient(
    vpc.VpcClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.RemoveVpcExtendCidrRequest{}
request.VpcId = "{vpc_id}"
var listExtendCidrsVpc = []string{
    "23.8.0.0/16",
}
vpcbody := &model.RemoveExtendCidrOption{
    ExtendCidrs: listExtendCidrsVpc,
}
request.Body = &model.RemoveVpcExtendCidrRequestBody{
    Vpc: vpcbody,
}
response, err := client.RemoveVpcExtendCidr(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Normal response to the PUT operation. For more status codes, see Status Code .
202	Normal response to the specified preflight request of API V3. For more status codes, see Status Code .

Error Codes

See [Error Codes](#).

5.2 Security Group

5.2.1 Creating a Security Group

Function

A security group is a collection of access control rules for cloud instances, such as cloud servers, containers, and databases, that have the same security requirements and that are mutually trusted within a VPC. You can define different access control rules for a security group, and these rules are then applied to all the instances added to this security group.

Constraints

By default, a security group only allows instances in it to communicate with each other.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v3/{project_id}/vpc/security-groups

Table 5-29 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	- Definition: ID of the project that a security group belongs to. For details about how to obtain a project ID, see Obtaining a Project ID. - Range: None

Request Parameters

Table 5-30 Request body parameters

Parameter	Mandatory	Type	Description
dry_run	No	Boolean	• Definition: Whether to only send the check request. • Constraints: None • Range: – true: A check request will be sent and no security group will be created. Check items include mandatory parameters, request format, and constraints. If the check fails, an error will be returned. If the check succeeds, response code 202 will be returned. – false: A request will be sent and a security group will be created. • Default Value: false
security_group	Yes	CreateSecurityGroupOption object	• Definition: Request body for creating a security group. • Constraints: None • Range: None • Default Value: None

Table 5-31 CreateSecurityGroupOption

Parameter	Mandatory	Type	Description
name	Yes	String	• Definition: Name of a security group. • Constraints: The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.). • Range: None • Default Value: None

Parameter	Mandatory	Type	Description
description	No	String	• Definition: Description of a security group. • Constraints: The value can contain no more than 255 characters and cannot contain angle brackets (< or >). • Range: None • Default Value: None
enterprise_project_id	No	String	• Definition: ID of the enterprise project that a security group belongs to. • Constraints: – The value can contain a maximum of 36 bytes. – The value is 0 or a string in UUID format with hyphens (-). • Range: None • Default Value: 0 (default enterprise project)
tags	No	Array of RequestTag objects	• Definition: Tags of a security group, including tag keys and tag values, which can be used to classify and identify resources. For details, see the tag objects. • Constraints: A maximum of 20 tag key-value pairs are supported. • Range: None • Default Value: None

Table 5-32 RequestTag

Parameter	Mandatory	Type	Description
key	Yes	String	Definition: Tag key. Constraints: N/A Range: - A tag key can contain a maximum of 128 Unicode characters and cannot be left blank. - Each tag key of a resource must be unique. - The value can contain: - Letters - Digits - Special characters: underscores (_), hyphens (-) - Chinese characters Default Value: N/A
value	Yes	String	Definition: Tag value. Constraints: N/A Range: - Each value can contain a maximum of 255 Unicode characters and can be left blank. - The value can contain: - Letters - Digits - Special characters: underscores (_), hyphens (-), periods (.) - Chinese characters Default Value: N/A

Response Parameters

Status code: 201

Table 5-33 Response body parameters

Parameter	Type	Description
request_id	String	- Definition: Request ID. - Range: None
security_group	SecurityGroupInfo object	- Definition: Response body for creating a security group. - Range: None

Table 5-34 SecurityGroupInfo

Parameter	Type	Description
id	String	- Definition: ID of a security group. After a security group is created, a security group ID is generated, which uniquely identifies the security group. - Range: The value is in UUID format with hyphens (-).
name	String	- Definition: Name of a security group. - Range: The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	- Definition: Description of a security group. - Range: The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
project_id	String	- Definition: ID of the project that a security group belongs to. - Range: None
created_at	String	- Definition: Time when a security group was created. - Range: UTC time in the format of yyyy-MM-ddTHH:mm:ssZ

Parameter	Type	Description
updated_at	String	- Definition: Time when a security group was updated. - Range: UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
enterprise_project_id	String	- Definition: ID of the enterprise project that a security group belongs to. - Range: The value is 0 or a string that contains a maximum of 36 characters in UUID format with hyphens (-). 0 indicates the default enterprise project.
tags	Array of ResponseTag objects	- Definition: Tags of a security group, including tag keys and tag values, which can be used to classify and identify resources. For details, see the tag objects. - Range: None
security_group_rules	Array of SecurityGroupRule objects	- Definition: Security group rule list. - Range: None

Table 5-35 ResponseTag

Parameter	Type	Description
key	String	Definition: Tag key. Range: - A tag key can contain a maximum of 128 Unicode characters and cannot be left blank. - Each tag key of a resource must be unique. - The value can contain: - Letters - Digits - Special characters: underscores (_), hyphens (-) - Chinese characters

Parameter	Type	Description
value	String	Definition: Tag value. Range: - Each value can contain a maximum of 255 Unicode characters and can be left blank. - The value can contain: - Letters - Digits - Special characters: underscores (_), hyphens (-), periods (.) - Chinese characters

Table 5-36 SecurityGroupRule

Parameter	Type	Description
id	String	- Definition: ID of a security group rule. After a security group rule is created, a security group rule ID is generated, which uniquely identifies the security group rule. - Range: The value is in UUID format with hyphens (-).
description	String	- Definition: Description of a security group rule. - Range: The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
security_group_id	String	- Definition: ID of the security group that a security group rule belongs to. - Range: None
direction	String	- Definition: Inbound or outbound direction of a security group rule. - Range: ingress: inbound direction egress: outbound direction

Parameter	Type	Description
protocol	String	• Definition: Communication protocol of a security group rule. • Range: – icmp – tcp – udp – icmpv6 – IP protocol number
ethertype	String	• Definition: IP address version of a security group rule. • Range: – IPv4 – IPv6
multiport	String	• Definition: Port range of a security group rule. • 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	• Definition: Action of a security group rule. • Range: – allow – deny
priority	Integer	• Definition: Priority of a security group rule. • Range: The value is from 1 to 100. The value 1 indicates the highest priority.
remote_group_id	String	• Definition: ID of the remote security group of a security group rule. If the action of the rule is allow, the traffic from the remote security group is allowed. If the action of the rule is deny, the traffic from the remote security group is denied. • Range: ID of an existing security group.

Parameter	Type	Description
remote_ip_prefix	String	- Definition: Remote IP address of a security group rule. - If direction is set to egress, the IP address is the outbound destination and will be accessed by instances in the security group. - If direction is set to ingress, the IP address is the inbound source and will access the instances in the security group. - Range: CIDR notation format. If an IP address is transferred in the request, the IP address is automatically formatted with /32 as the subnet mask, for example, 192.168.21.45/32.
remote_address_group_id	String	- Definition: ID of the remote IP address group of a security group rule. - Range: ID of an existing IP address group.
created_at	String	- Definition: Time when a security group rule was created. - Range: UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
updated_at	String	- Definition: Time when a security group rule was updated. - Range: UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
project_id	String	- Definition: ID of the project that a security group rule belongs to. - Range: None
enabled	Boolean	- Definition: Whether to enable a security group rule. - Range: true: The security group rule is enabled. false: The security group rule is disabled.

Status code: 202

Table 5-37 Response body parameters

Parameter	Type	Description
request_id	String	- Definition: Request ID. - Range: None
error_msg	String	- Definition: Error message. - Range: None
error_code	String	- Definition: Error code. - Range: None

Example Requests

- Create a security group, set its name to **security_group_1** and description to **security group description**, and specify the request as a preflight request.

```
POST https://{Endpoint}/v3/{project_id}/vpc/security-groups
```

```
{
  "security_group": {
    "name": "security_group_1",
    "description": "security group description"
  },
  "dry_run": true
}
```

- 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"
  }
}
```

Example Responses

Status code: 201

Normal response to the POST operation. For more status codes, see [Status Code](#).

- ```
{
 "security_group": {
 "id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
 "name": "security_group_1",
 "project_id": "060576782980d5762f9ec014dd2f1148",
 "description": "security group description",
 "enterprise_project_id": "0",
 "tags": [],
 "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,
"enabled" : true
}, {
 "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,
 "enabled" : true
}, {
 "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,
 "enabled" : true
}, {
 "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,
 "enabled" : true
}],
"created_at" : "2020-07-09T05:56:27Z",
"updated_at" : "2020-07-09T05:56:27Z"
},
"request_id" : "a8cf4f79ca3c22ca685e7e8872e8c20b"
}
```

**Status code: 202**



Normal response for the specified pre-check request of API V3. For more status codes, see [Status Code](#).

```
{
 "error_msg": "Request validation has been passed with dry run...",
 "error_code": "SYS.0202",
 "request_id": "cfd81aea3f59eac7128dba4b36d516c8"
}
```

## SDK Sample Code

The SDK sample code is as follows.

### Java

- Create a security group, set its name to **security\_group\_1** and description to **security group description**, and specify the request as a preflight request.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class CreateSecurityGroupSolution {

 public static void main(String[] args) {
 // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
 // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
 // environment variables and decrypted during use to ensure security.
 // In this example, AK and SK are stored in environment variables for authentication. Before
 // running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local
 // environment
 String ak = System.getenv("CLOUD_SDK_AK");
 String sk = System.getenv("CLOUD_SDK_SK");
 String projectId = "{project_id}";

 ICredential auth = new BasicCredentials()
 .withProjectId(projectId)
 .withAk(ak)
 .withSk(sk);

 VpcClient client = VpcClient.newBuilder()
 .withCredential(auth)
 .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
 .build();
 CreateSecurityGroupRequest request = new CreateSecurityGroupRequest();
 CreateSecurityGroupRequestBody body = new CreateSecurityGroupRequestBody();
 CreateSecurityGroupOption securityGroupbody = new CreateSecurityGroupOption();
 securityGroupbody.setName("security_group_1")
 .withDescription("security group description");
 body.withSecurityGroup(securityGroupbody);
 body.withDryRun(true);
 request.withBody(body);
 try {
 CreateSecurityGroupResponse response = client.createSecurityGroup(request);
 System.out.println(response.toString());
 } catch (ConnectionException e) {
 e.printStackTrace();
 } catch (RequestTimeoutException e) {
 e.printStackTrace();
 } catch (ServiceResponseException e) {
 e.printStackTrace();
 }
 }
}
```

```
 e.printStackTrace();
 System.out.println(e.getHttpStatusCode());
 System.out.println(e.getRequestId());
 System.out.println(e.getErrorCode());
 System.out.println(e.getErrorMsg());
 }
}
```

- Create a security group and set its name to *security\_group\_1\** and description to **security group description**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class CreateSecurityGroupSolution {

 public static void main(String[] args) {
 // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
 // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
 // environment variables and decrypted during use to ensure security.
 // In this example, AK and SK are stored in environment variables for authentication. Before
 // running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local
 // environment
 String ak = System.getenv("CLOUD_SDK_AK");
 String sk = System.getenv("CLOUD_SDK_SK");
 String projectId = "{project_id}";

 ICredential auth = new BasicCredentials()
 .withProjectId(projectId)
 .withAk(ak)
 .withSk(sk);

 VpcClient client = VpcClient.newBuilder()
 .withCredential(auth)
 .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
 .build();
 CreateSecurityGroupRequest request = new CreateSecurityGroupRequest();
 CreateSecurityGroupRequestBody body = new CreateSecurityGroupRequestBody();
 CreateSecurityGroupOption securityGroupbody = new CreateSecurityGroupOption();
 securityGroupbody.setName("security_group_1")
 .withDescription("security group description");
 body.withSecurityGroup(securityGroupbody);
 request.withBody(body);
 try {
 CreateSecurityGroupResponse response = client.createSecurityGroup(request);
 System.out.println(response.toString());
 } catch (ConnectionException e) {
 e.printStackTrace();
 } catch (RequestTimeoutException e) {
 e.printStackTrace();
 } catch (ServiceResponseException e) {
 e.printStackTrace();
 System.out.println(e.getHttpStatusCode());
 System.out.println(e.getRequestId());
 System.out.println(e.getErrorCode());
 System.out.println(e.getErrorMsg());
 }
 }
}
```

## Python

- Create a security group, set its name to **security\_group\_1** and description to **security group description**, and specify the request as a preflight request.

```
coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
 # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
 # security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
 # environment variables and decrypted during use to ensure security.
 # In this example, AK and SK are stored in environment variables for authentication. Before
 # running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local
 # environment
 ak = os.environ["CLOUD_SDK_AK"]
 sk = os.environ["CLOUD_SDK_SK"]
 projectId = "{project_id}"

 credentials = BasicCredentials(ak, sk, projectId)

 client = VpcClient.new_builder() \
 .with_credentials(credentials) \
 .with_region(VpcRegion.value_of("<YOUR REGION>")) \
 .build()

 try:
 request = CreateSecurityGroupRequest()
 securityGroupbody = CreateSecurityGroupOption(
 name="security_group_1",
 description="security group description"
)
 request.body = CreateSecurityGroupRequestBody(
 security_group=securityGroupbody,
 dry_run=True
)
 response = client.create_security_group(request)
 print(response)
 except exceptions.ClientRequestException as e:
 print(e.status_code)
 print(e.request_id)
 print(e.error_code)
 print(e.error_msg)
```

- Create a security group and set its name to *security\_group\_1\** and description to **security group description**.

```
coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
 # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
 # security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
 # environment variables and decrypted during use to ensure security.
 # In this example, AK and SK are stored in environment variables for authentication. Before
 # running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local
 # environment
 ak = os.environ["CLOUD_SDK_AK"]
 sk = os.environ["CLOUD_SDK_SK"]
 projectId = "{project_id}"
```

```
credentials = BasicCredentials(ak, sk, projectId)

client = VpcClient.new_builder() \
 .with_credentials(credentials) \
 .with_region(VpcRegion.value_of("<YOUR REGION>")) \
 .build()

try:
 request = CreateSecurityGroupRequest()
 securityGroupbody = CreateSecurityGroupOption(
 name="security_group_1",
 description="security group description"
)
 request.body = CreateSecurityGroupRequestBody(
 security_group=securityGroupbody
)
 response = client.create_security_group(request)
 print(response)
except exceptions.ClientRequestException as e:
 print(e.status_code)
 print(e.request_id)
 print(e.error_code)
 print(e.error_msg)
```

## Go

- Create a security group, set its name to **security\_group\_1** and description to **security group description**, and specify the request as a preflight request.

```
package main

import (
 "fmt"
 "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
 vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
 "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
 region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
 // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
 // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
 // environment variables and decrypted during use to ensure security.
 // In this example, AK and SK are stored in environment variables for authentication. Before
 // running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local
 // environment
 ak := os.Getenv("CLOUD_SDK_AK")
 sk := os.Getenv("CLOUD_SDK_SK")
 projectId := "{project_id}"

 auth := basic.NewCredentialsBuilder().
 WithAk(ak).
 WithSk(sk).
 WithProjectId(projectId).
 Build()

 client := vpc.NewVpcClient(
 vpc.VpcClientBuilder().
 WithRegion(region.ValueOf("<YOUR REGION>")).
 WithCredential(auth).
 Build())

 request := &model.CreateSecurityGroupRequest{
 descriptionSecurityGroup:= "security group description"
 securityGroupbody := &model.CreateSecurityGroupOption{
 Name: "security_group_1",
 Description: &descriptionSecurityGroup,
 }
 }
```

```
dryRunCreateSecurityGroupRequestBody:= true
request.Body = &model.CreateSecurityGroupRequestBody{
 SecurityGroup: securityGroupbody,
 DryRun: &dryRunCreateSecurityGroupRequestBody,
}
response, err := client.CreateSecurityGroup(request)
if err == nil {
 fmt.Printf("%+v\n", response)
} else {
 fmt.Println(err)
}
}
```

- Create a security group and set its name to *security\_group\_1\** and description to **security group description**.

```
package main

import (
 "fmt"
 "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
 vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
 "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
 region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
 // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
 // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
 // environment variables and decrypted during use to ensure security.
 // In this example, AK and SK are stored in environment variables for authentication. Before
 // running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local
 // environment
 ak := os.Getenv("CLOUD_SDK_AK")
 sk := os.Getenv("CLOUD_SDK_SK")
 projectId := "{project_id}"

 auth := basic.NewCredentialsBuilder().
 WithAk(ak).
 WithSk(sk).
 WithProjectId(projectId).
 Build()

 client := vpc.NewVpcClient(
 vpc.VpcClientBuilder().
 WithRegion(region.ValueOf("<YOUR REGION>")).
 WithCredential(auth).
 Build())

 request := &model.CreateSecurityGroupRequest{
 descriptionSecurityGroup:= "security group description"
 securityGroupbody := &model.CreateSecurityGroupOption{
 Name: "security_group_1",
 Description: &descriptionSecurityGroup,
 }
 }
 request.Body = &model.CreateSecurityGroupRequestBody{
 SecurityGroup: securityGroupbody,
 }
 response, err := client.CreateSecurityGroup(request)
 if err == nil {
 fmt.Printf("%+v\n", response)
 } else {
 fmt.Println(err)
 }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description                                                                                                             |
|-------------|-------------------------------------------------------------------------------------------------------------------------|
| 201         | Normal response to the POST operation. For more status codes, see <a href="#">Status Code</a> .                         |
| 202         | Normal response for the specified pre-check request of API V3. For more status codes, see <a href="#">Status Code</a> . |

## Error Codes

See [Error Codes](#).

## 5.2.2 Querying Security Groups

### Function

After a security group is created, you can call this API to query all information about the security group, including the name, ID, and description.

### Constraints

You can query all security groups under your account. A maximum of 2,000 records can be returned for each query. If the number of records exceeds 2,000, the pagination marker will be returned.

### Calling Method

For details, see [Calling APIs](#).

### URI

GET /v3/{project\_id}/vpc/security-groups

**Table 5-38** Path Parameters

| Parameter  | Mandatory | Type   | Description                                                                                                                                                                                                                   |
|------------|-----------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| project_id | Yes       | String | <ul style="list-style-type: none"><li>Definition: ID of the project that a security group belongs to. For details about how to obtain a project ID, see <a href="#">Obtaining a Project ID</a>.</li><li>Range: None</li></ul> |

**Table 5-39** Query Parameters

| Parameter | Mandatory | Type             | Description                                                                                                                                                                                                                            |
|-----------|-----------|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| limit     | No        | Integer          | <ul style="list-style-type: none"><li>Definition: Number of resources returned on each page.</li><li>Range: 0-2000</li></ul>                                                                                                           |
| marker    | No        | String           | <ul style="list-style-type: none"><li>Definition: ID of the resource from which the pagination query starts. If the parameter is left blank, only resources on the first page are queried.</li><li>Range: Security group ID.</li></ul> |
| id        | No        | Array of strings | <ul style="list-style-type: none"><li>Definition: ID of a security group. This field can be used to precisely filter security groups. Multiple IDs can be specified for filtering.</li><li>Range: None</li></ul>                       |
| name      | No        | Array of strings | <ul style="list-style-type: none"><li>Definition: Name of a security group. This field can be used to precisely filter security groups. Multiple names can be specified for filtering.</li><li>Range: None</li></ul>                   |

| Parameter             | Mandatory | Type             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------|-----------|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| description           | No        | Array of strings | <ul style="list-style-type: none"><li>Definition: Description of a security group. This field can be used to precisely filter security groups. Multiple descriptions can be specified for filtering.</li><li>Range: None</li></ul>                                                                                                                                                                                                                                                                                                                                                                     |
| enterprise_project_id | No        | String           | <ul style="list-style-type: none"><li>Definition: ID of the enterprise project that a security group belongs to. This field can be used to filter the security groups associated with an enterprise project.</li><li>Range:<ul style="list-style-type: none"><li>The value is <b>0</b> or a string that contains a maximum of 36 characters in UUID format with hyphens (-). <b>0</b> indicates the default enterprise project.</li><li>To obtain the security groups associated with all enterprise projects that a user has permissions to view, specify <b>all_granted_eps</b>.</li></ul></li></ul> |

Request Parameters

None

Response Parameters

Status code: 200

Table 5-40 Response body parameters

| Parameter       | Type                                  | Description                                                                                                                 |
|-----------------|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| security_groups | Array of <b>SecurityGroup</b> objects | <ul style="list-style-type: none"><li>Definition: Response body for querying security groups.</li><li>Range: None</li></ul> |



| Parameter  | Type                            | Description                                                                                             |
|------------|---------------------------------|---------------------------------------------------------------------------------------------------------|
| request_id | String                          | <ul style="list-style-type: none"><li>Definition: Request ID.</li><li>Range: None</li></ul>             |
| page_info  | <a href="#">PageInfo</a> object | <ul style="list-style-type: none"><li>Definition: Pagination information.</li><li>Range: None</li></ul> |

**Table 5-41** SecurityGroup

| Parameter   | Type   | Description                                                                                                                                                                                                                                                         |
|-------------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| id          | String | <ul style="list-style-type: none"><li>Definition: ID of a security group. After a security group is created, a security group ID is generated, which uniquely identifies the security group.</li><li>Range: The value is in UUID format with hyphens (-).</li></ul> |
| name        | String | <ul style="list-style-type: none"><li>Definition: Name of a security group.</li><li>Range: The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).</li></ul>                                            |
| description | String | <ul style="list-style-type: none"><li>Definition: Description of a security group.</li><li>Range: The value can contain no more than 255 characters and cannot contain angle brackets (&lt; or &gt;).</li></ul>                                                     |
| project_id  | String | <ul style="list-style-type: none"><li>Definition: ID of the project that a security group belongs to.</li><li>Range: None</li></ul>                                                                                                                                 |
| created_at  | String | <ul style="list-style-type: none"><li>Definition: Time when a security group was created.</li><li>Range: UTC time in the format of yyyy-MM-ddTHH:mm:ssZ</li></ul>                                                                                                   |
| updated_at  | String | <ul style="list-style-type: none"><li>Definition: Time when a security group was updated.</li><li>Range: UTC time in the format of yyyy-MM-ddTHH:mm:ssZ</li></ul>                                                                                                   |

| Parameter             | Type                                         | Description                                                                                                                                                                                                                                                                                              |
|-----------------------|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| enterprise_project_id | String                                       | <ul style="list-style-type: none"><li>Definition: ID of the enterprise project that a security group belongs to.</li><li>Range: The value is <b>0</b> or a string that contains a maximum of 36 characters in UUID format with hyphens (-). <b>0</b> indicates the default enterprise project.</li></ul> |
| tags                  | Array of <a href="#">ResponseTag</a> objects | <ul style="list-style-type: none"><li>Definition: Tags of a security group, including tag keys and tag values, which can be used to classify and identify resources. For details, see the tag objects.</li><li>Range: None</li></ul>                                                                     |

**Table 5-42** ResponseTag

| Parameter | Type   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| key       | String | <p><b>Definition:</b><br/>Tag key.</p> <p><b>Range:</b></p> <ul style="list-style-type: none"><li>A tag key can contain a maximum of 128 Unicode characters and cannot be left blank.</li><li>Each tag key of a resource must be unique.</li><li>The value can contain:<ul style="list-style-type: none"><li>Letters</li><li>Digits</li><li>Special characters: underscores (_), hyphens (-)</li><li>Chinese characters</li></ul></li></ul> |

| Parameter | Type   | Description                                                                                                                                                                                                                                                                                                                                                                               |
|-----------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| value     | String | <b>Definition:</b><br>Tag value.<br><b>Range:</b> <ul style="list-style-type: none"><li>Each value can contain a maximum of 255 Unicode characters and can be left blank.</li><li>The value can contain:<ul style="list-style-type: none"><li>Letters</li><li>Digits</li><li>Special characters: underscores (_), hyphens (-), periods (.)</li><li>Chinese characters</li></ul></li></ul> |

**Table 5-43** PageInfo

| Parameter       | Type    | Description                                                                                                                                                 |
|-----------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| previous_marker | String  | <b>Definition:</b><br>The first record on the current page.<br><b>Range:</b><br>N/A                                                                         |
| current_count   | Integer | <b>Definition:</b><br>Total number of resources on the current page.<br><b>Range:</b><br>N/A                                                                |
| next_marker     | String  | <b>Definition:</b><br>The last record on the current page. The <b>next_marker</b> field does not exist if the page is the last one.<br><b>Range:</b><br>N/A |

## Example Requests

Querying security groups

```
GET https://{Endpoint}/v3/{project_id}/vpc/security-groups
```

## Example Responses

**Status code: 200**

Normal response to the GET operation. For more status codes, see [Status Codes](#).

```
{
 "request_id": "d31cb32ca06f3c1a294fa24e6cbc5a56",
 "security_groups": [{
 "id": "0552091e-b83a-49dd-88a7-4a5c86fd9ec3",
 "name": "sg-test",
 "project_id": "060576782980d5762f9ec014dd2f1148",
 "description": "test",
 "enterprise_project_id": 0,
 "created_at": "2019-10-16T11:11:14.000+00:00",
 "updated_at": "2020-03-25T10:53:46.000+00:00",
 "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": "2019-12-03T09:02:11.000+00:00",
 "updated_at": "2019-12-03T09:02:11.000+00:00",
 "tags": []
 }],
 "page_info": {
 "previous_marker": "0552091e-b83a-49dd-88a7-4a5c86fd9ec3",
 "current_count": 2
 }
}
```

## SDK Sample Code

The SDK sample code is as follows.

### Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class ListSecurityGroupsSolution {

 public static void main(String[] args) {
 // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
 // In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
 String ak = System.getenv("CLOUD_SDK_AK");
 String sk = System.getenv("CLOUD_SDK_SK");
 String projectId = "{project_id}";

 ICredential auth = new BasicCredentials()
 .withProjectId(projectId)
 .withAk(ak)
 .withSk(sk);

 VpcClient client = VpcClient.newBuilder()
 .withCredential(auth)
```

```
 .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
 .build();
ListSecurityGroupsRequest request = new ListSecurityGroupsRequest();
try {
 ListSecurityGroupsResponse response = client.listSecurityGroups(request);
 System.out.println(response.toString());
} catch (ConnectionException e) {
 e.printStackTrace();
} catch (RequestTimeoutException e) {
 e.printStackTrace();
} catch (ServiceResponseException e) {
 e.printStackTrace();
 System.out.println(e.getHttpStatusCode());
 System.out.println(e.getRequestId());
 System.out.println(e.getErrorCode());
 System.out.println(e.getErrorMsg());
}
}
```

## Python

```
coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
 # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
 # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
 # variables and decrypted during use to ensure security.
 # In this example, AK and SK are stored in environment variables for authentication. Before running this
 # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
 ak = os.environ["CLOUD_SDK_AK"]
 sk = os.environ["CLOUD_SDK_SK"]
 projectId = "{project_id}"

 credentials = BasicCredentials(ak, sk, projectId)

 client = VpcClient.new_builder() \
 .with_credentials(credentials) \
 .with_region(VpcRegion.valueOf("<YOUR REGION>")) \
 .build()

 try:
 request = ListSecurityGroupsRequest()
 response = client.list_security_groups(request)
 print(response)
 except exceptions.ClientRequestException as e:
 print(e.status_code)
 print(e.request_id)
 print(e.error_code)
 print(e.error_msg)
```

## Go

```
package main

import (
 "fmt"
 "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
 vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
 "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
 region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)
```

```
func main() {
 // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
 // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
 // variables and decrypted during use to ensure security.
 // In this example, AK and SK are stored in environment variables for authentication. Before running this
 // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
 ak := os.Getenv("CLOUD_SDK_AK")
 sk := os.Getenv("CLOUD_SDK_SK")
 projectId := "{project_id}"

 auth := basic.NewCredentialsBuilder().
 WithAk(ak).
 WithSk(sk).
 WithProjectId(projectId).
 Build()

 client := vpc.NewVpcClient(
 vpc.VpcClientBuilder().
 WithRegion(region.ValueOf("<YOUR REGION>")).
 WithCredential(auth).
 Build())

 request := &model.ListSecurityGroupsRequest{}
 response, err := client.ListSecurityGroups(request)
 if err == nil {
 fmt.Printf("%+v\n", response)
 } else {
 fmt.Println(err)
 }
}
```

## More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

## Status Codes

| Status Code | Description                                                                                     |
|-------------|-------------------------------------------------------------------------------------------------|
| 200         | Normal response to the GET operation. For more status codes, see <a href="#">Status Codes</a> . |

## Error Codes

See [Error Codes](#).

## 5.2.3 Querying the Details of a Security Group

### Function

After a security group is created, you can call this API to query all information about the security group, including the name, ID, and description.

### Calling Method

For details, see [Calling APIs](#).

## URI

GET /v3/{project\_id}/vpc/security-groups/{security\_group\_id}

**Table 5-44** Path Parameters

| Parameter         | Mandatory | Type   | Description                                                                                                                                                                                                                   |
|-------------------|-----------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| project_id        | Yes       | String | <ul style="list-style-type: none"><li>Definition: ID of the project that a security group belongs to. For details about how to obtain a project ID, see <a href="#">Obtaining a Project ID</a>.</li><li>Range: None</li></ul> |
| security_group_id | Yes       | String | <ul style="list-style-type: none"><li>Definition: ID of a security group.</li><li>Range: None</li></ul>                                                                                                                       |

## Request Parameters

None

## Response Parameters

**Status code: 200**

**Table 5-45** Response body parameters

| Parameter      | Type                                     | Description                                                                                                                                |
|----------------|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| request_id     | String                                   | <ul style="list-style-type: none"><li>Definition: Request ID.</li><li>Range: None</li></ul>                                                |
| security_group | <a href="#">SecurityGroupInfo</a> object | <ul style="list-style-type: none"><li>Definition: Response body for querying details about a security group.</li><li>Range: None</li></ul> |

**Table 5-46** SecurityGroupInfo

| Parameter             | Type   | Description                                                                                                                                                                                                                                                                                              |
|-----------------------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| id                    | String | <ul style="list-style-type: none"><li>Definition: ID of a security group. After a security group is created, a security group ID is generated, which uniquely identifies the security group.</li><li>Range: The value is in UUID format with hyphens (-).</li></ul>                                      |
| name                  | String | <ul style="list-style-type: none"><li>Definition: Name of a security group.</li><li>Range: The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).</li></ul>                                                                                 |
| description           | String | <ul style="list-style-type: none"><li>Definition: Description of a security group.</li><li>Range: The value can contain no more than 255 characters and cannot contain angle brackets (&lt; or &gt;).</li></ul>                                                                                          |
| project_id            | String | <ul style="list-style-type: none"><li>Definition: ID of the project that a security group belongs to.</li><li>Range: None</li></ul>                                                                                                                                                                      |
| created_at            | String | <ul style="list-style-type: none"><li>Definition: Time when a security group was created.</li><li>Range: UTC time in the format of yyyy-MM-ddTHH:mm:ssZ</li></ul>                                                                                                                                        |
| updated_at            | String | <ul style="list-style-type: none"><li>Definition: Time when a security group was updated.</li><li>Range: UTC time in the format of yyyy-MM-ddTHH:mm:ssZ</li></ul>                                                                                                                                        |
| enterprise_project_id | String | <ul style="list-style-type: none"><li>Definition: ID of the enterprise project that a security group belongs to.</li><li>Range: The value is <b>0</b> or a string that contains a maximum of 36 characters in UUID format with hyphens (-). <b>0</b> indicates the default enterprise project.</li></ul> |



| Parameter            | Type                                               | Description                                                                                                                                                                                                                          |
|----------------------|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| tags                 | Array of <a href="#">ResponseTag</a> objects       | <ul style="list-style-type: none"><li>Definition: Tags of a security group, including tag keys and tag values, which can be used to classify and identify resources. For details, see the tag objects.</li><li>Range: None</li></ul> |
| security_group_rules | Array of <a href="#">SecurityGroupRule</a> objects | <ul style="list-style-type: none"><li>Definition: Security group rule list.</li><li>Range: None</li></ul>                                                                                                                            |

**Table 5-47** ResponseTag

| Parameter | Type   | Description                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| key       | String | <b>Definition:</b><br>Tag key.<br><b>Range:</b> <ul style="list-style-type: none"><li>A tag key can contain a maximum of 128 Unicode characters and cannot be left blank.</li><li>Each tag key of a resource must be unique.</li><li>The value can contain:<ul style="list-style-type: none"><li>Letters</li><li>Digits</li><li>Special characters: underscores (_), hyphens (-)</li><li>Chinese characters</li></ul></li></ul> |
| value     | String | <b>Definition:</b><br>Tag value.<br><b>Range:</b> <ul style="list-style-type: none"><li>Each value can contain a maximum of 255 Unicode characters and can be left blank.</li><li>The value can contain:<ul style="list-style-type: none"><li>Letters</li><li>Digits</li><li>Special characters: underscores (_), hyphens (-), periods (.)</li><li>Chinese characters</li></ul></li></ul>                                       |

**Table 5-48** SecurityGroupRule

| Parameter         | Type   | Description                                                                                                                                                                                                                                                                             |
|-------------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| id                | String | <ul style="list-style-type: none"><li>Definition: ID of a security group rule. After a security group rule is created, a security group rule ID is generated, which uniquely identifies the security group rule.</li><li>Range: The value is in UUID format with hyphens (-).</li></ul> |
| description       | String | <ul style="list-style-type: none"><li>Definition: Description of a security group rule.</li><li>Range: The value can contain no more than 255 characters and cannot contain angle brackets (&lt; or &gt;).</li></ul>                                                                    |
| security_group_id | String | <ul style="list-style-type: none"><li>Definition: ID of the security group that a security group rule belongs to.</li><li>Range: None</li></ul>                                                                                                                                         |
| direction         | String | <ul style="list-style-type: none"><li>Definition: Inbound or outbound direction of a security group rule.</li><li>Range:<ul style="list-style-type: none"><li>– <b>ingress</b>: inbound direction</li><li>– <b>egress</b>: outbound direction</li></ul></li></ul>                       |
| protocol          | String | <ul style="list-style-type: none"><li>Definition: Communication protocol of a security group rule.</li><li>Range:<ul style="list-style-type: none"><li>– <b>icmp</b></li><li>– <b>tcp</b></li><li>– <b>udp</b></li><li>– <b>icmpv6</b></li><li>– IP protocol number</li></ul></li></ul> |
| ethertype         | String | <ul style="list-style-type: none"><li>Definition: IP address version of a security group rule.</li><li>Range:<ul style="list-style-type: none"><li>– IPv4</li><li>– IPv6</li></ul></li></ul>                                                                                            |

| Parameter        | Type    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| multiport        | String  | <ul style="list-style-type: none"><li>Definition: Port range of a security group rule.</li><li>Range: The value can be a single port (80), a port range (1-30), or inconsecutive ports separated by commas (22,3389,80).</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                     |
| action           | String  | <ul style="list-style-type: none"><li>Definition: Action of a security group rule.</li><li>Range:<ul style="list-style-type: none"><li>– <b>allow</b></li><li>– <b>deny</b></li></ul></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| priority         | Integer | <ul style="list-style-type: none"><li>Definition: Priority of a security group rule.</li><li>Range: The value is from 1 to 100. The value 1 indicates the highest priority.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| remote_group_id  | String  | <ul style="list-style-type: none"><li>Definition: ID of the remote security group of a security group rule. If the action of the rule is <b>allow</b>, the traffic from the remote security group is allowed. If the action of the rule is <b>deny</b>, the traffic from the remote security group is denied.</li><li>Range: ID of an existing security group.</li></ul>                                                                                                                                                                                                                                                                               |
| remote_ip_prefix | String  | <ul style="list-style-type: none"><li>Definition: Remote IP address of a security group rule.<ul style="list-style-type: none"><li>– If <b>direction</b> is set to <b>egress</b>, the IP address is the outbound destination and will be accessed by instances in the security group.</li><li>– If <b>direction</b> is set to <b>ingress</b>, the IP address is the inbound source and will access the instances in the security group.</li></ul></li><li>Range: CIDR notation format. If an IP address is transferred in the request, the IP address is automatically formatted with /32 as the subnet mask, for example, 192.168.21.45/32.</li></ul> |

| Parameter               | Type    | Description                                                                                                                                                                                                                                                                    |
|-------------------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| remote_address_group_id | String  | <ul style="list-style-type: none"><li>Definition: ID of the remote IP address group of a security group rule.</li><li>Range: ID of an existing IP address group.</li></ul>                                                                                                     |
| created_at              | String  | <ul style="list-style-type: none"><li>Definition: Time when a security group rule was created.</li><li>Range: UTC time in the format of yyyy-MM-ddTHH:mm:ssZ</li></ul>                                                                                                         |
| updated_at              | String  | <ul style="list-style-type: none"><li>Definition: Time when a security group rule was updated.</li><li>Range: UTC time in the format of yyyy-MM-ddTHH:mm:ssZ</li></ul>                                                                                                         |
| project_id              | String  | <ul style="list-style-type: none"><li>Definition: ID of the project that a security group rule belongs to.</li><li>Range: None</li></ul>                                                                                                                                       |
| enabled                 | Boolean | <ul style="list-style-type: none"><li>Definition: Whether to enable a security group rule.</li><li>Range:<ul style="list-style-type: none"><li><b>true</b>: The security group rule is enabled.</li><li><b>false</b>: The security group rule is disabled.</li></ul></li></ul> |

## Example Requests

Querying the details of a security group

```
GET https://{Endpoint}/v3/{project_id}/vpc/security-groups/69c999ad-d9ef-4d79-94fd-35e6ceb75325
```

## Example Responses

**Status code: 200**

Normal response to the GET operation. For more status codes, see [Status Codes](#).

- ```
{
  "security_group": {
    "id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
    "name": "security_group_1",
    "project_id": "060576782980d5762f9ec014dd2f1148",
    "description": "security group description",
    "enterprise_project_id": 0,
    "tags": [ {
      "key": "a",
      "value": "b"
    } ],
    "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",
"description": "",
"created_at": "2020-07-09T05:56:27.000+00:00",
"updated_at": "2020-07-09T05:56:27.000+00:00",
"ethertype": "IPv6",
"action": "allow",
"priority": 100,
"protocol": null,
"multiport": null,
"remote_ip_prefix": null,
"remote_address_group_id": null,
"enabled": true
}, {
  "id": "3d6480e8-9ea4-46dc-bb1b-8db190cd5677",
  "project_id": "060576782980d5762f9ec014dd2f1148",
  "security_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
  "direction": "egress",
  "description": "",
  "created_at": "2020-07-09T05:56:27.000+00:00",
  "updated_at": "2020-07-09T05:56:27.000+00:00",
  "ethertype": "IPv6",
  "action": "allow",
  "priority": 100,
  "protocol": null,
  "multiport": null,
  "remote_ip_prefix": null,
  "remote_group_id": null,
  "remote_address_group_id": null,
  "enabled": true
}, {
  "id": "9581f18c-1fdd-43da-ace9-7758a56ef28a",
  "project_id": "060576782980d5762f9ec014dd2f1148",
  "security_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
  "direction": "egress",
  "description": "",
  "created_at": "2020-07-09T05:56:27.000+00:00",
  "updated_at": "2020-07-09T05:56:27.000+00:00",
  "ethertype": "IPv4",
  "action": "allow",
  "priority": 100,
  "protocol": null,
  "multiport": null,
  "remote_ip_prefix": null,
  "remote_group_id": null,
  "remote_address_group_id": null,
  "enabled": true
}, {
  "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",
  "description": "",
  "created_at": "2020-07-09T05:56:27.000+00:00",
  "updated_at": "2020-07-09T05:56:27.000+00:00",
  "ethertype": "IPv4",
  "action": "allow",
  "priority": 100,
  "protocol": null,
  "multiport": null,
  "remote_ip_prefix": null,
  "remote_address_group_id": null,
  "enabled": true
} ],
"created_at": "2020-07-09T05:56:27.000+00:00",
"updated_at": "2020-07-09T05:56:27.000+00:00"
```

```
    },  
    "request_id" : "a8cf4f79ca3c22ca685e7e8872e8c20b"  
  }  
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;  
  
import com.huaweicloud.sdk.core.auth.ICredential;  
import com.huaweicloud.sdk.core.auth.BasicCredentials;  
import com.huaweicloud.sdk.core.exception.ConnectionException;  
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;  
import com.huaweicloud.sdk.core.exception.ServiceResponseException;  
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;  
import com.huaweicloud.sdk.vpc.v3.*;  
import com.huaweicloud.sdk.vpc.v3.model.*;  
  
public class ShowSecurityGroupSolution {  
    public static void main(String[] args) {  
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great  
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or  
        // environment variables and decrypted during use to ensure security.  
        // In this example, AK and SK are stored in environment variables for authentication. Before running  
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
        String ak = System.getenv("CLOUD_SDK_AK");  
        String sk = System.getenv("CLOUD_SDK_SK");  
        String projectId = "{project_id}";  
  
        ICredential auth = new BasicCredentials()  
            .withProjectId(projectId)  
            .withAk(ak)  
            .withSk(sk);  
  
        VpcClient client = VpcClient.newBuilder()  
            .withCredential(auth)  
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))  
            .build();  
        ShowSecurityGroupRequest request = new ShowSecurityGroupRequest();  
        request.withSecurityGroupId("{security_group_id}");  
        try {  
            ShowSecurityGroupResponse response = client.showSecurityGroup(request);  
            System.out.println(response.toString());  
        } catch (ConnectionException e) {  
            e.printStackTrace();  
        } catch (RequestTimeoutException e) {  
            e.printStackTrace();  
        } catch (ServiceResponseException e) {  
            e.printStackTrace();  
            System.out.println(e.getStatusCode());  
            System.out.println(e.getRequestId());  
            System.out.println(e.getErrorCode());  
            System.out.println(e.getErrorMsg());  
        }  
    }  
}
```

Python

```
# coding: utf-8  
  
import os
```

```
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowSecurityGroupRequest()
        request.security_group_id = "{security_group_id}"
        response = client.show_security_group(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowSecurityGroupRequest{
        request.SecurityGroupId = "{security_group_id}"
    }
```

```
response, err := client.ShowSecurityGroup(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Normal response to the GET operation. For more status codes, see Status Codes .

Error Codes

See [Error Codes](#).

5.2.4 Updating a Security Group

Function

After a security group is created, you can call this API to update basic information about the security group, including the name and description.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v3/{project_id}/vpc/security-groups/{security_group_id}

Table 5-49 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	- Definition: ID of the project that a security group belongs to. For details about how to obtain a project ID, see Obtaining a Project ID. - Range: None

Parameter	Mandatory	Type	Description
security_group_id	Yes	String	• Definition: ID of a security group. • Range: None

Request Parameters

Table 5-50 Request body parameters

Parameter	Mandatory	Type	Description
dry_run	No	Boolean	• Definition: Whether to only send the check request. • Constraints: None • Range: – true: A check request will be sent and no security group will be updated. Check items include mandatory parameters, request format, and constraints. If the check fails, an error will be returned. If the check succeeds, response code 202 will be returned. – false: A request will be sent and a security group will be updated. • Default Value: false
security_group	Yes	UpdateSecurityGroupOption object	• Definition: Request body for updating a security group. • Constraints: None • Range: None • Default Value: None

Table 5-51 UpdateSecurityGroupOption

Parameter	Mandatory	Type	Description
name	No	String	- Definition: Name of a security group. - Constraints: The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.). - Range: None - Default Value: None
description	No	String	- Definition: Description of a security group. - Constraints: The value can contain no more than 255 characters and cannot contain angle brackets (< or >). - Range: None - Default Value: None

Response Parameters

Status code: 200

Table 5-52 Response body parameters

Parameter	Type	Description
request_id	String	- Definition: Request ID. - Range: None
security_group	SecurityGroupInfo object	- Definition: Response body for updating a security group. - Range: None

Table 5-53 SecurityGroupInfo

Parameter	Type	Description
id	String	- Definition: ID of a security group. After a security group is created, a security group ID is generated, which uniquely identifies the security group. - Range: The value is in UUID format with hyphens (-).
name	String	- Definition: Name of a security group. - Range: The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	- Definition: Description of a security group. - Range: The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
project_id	String	- Definition: ID of the project that a security group belongs to. - Range: None
created_at	String	- Definition: Time when a security group was created. - Range: UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
updated_at	String	- Definition: Time when a security group was updated. - Range: UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
enterprise_project_id	String	- Definition: ID of the enterprise project that a security group belongs to. - Range: The value is 0 or a string that contains a maximum of 36 characters in UUID format with hyphens (-). 0 indicates the default enterprise project.

Parameter	Type	Description
tags	Array of ResponseTag objects	- Definition: Tags of a security group, including tag keys and tag values, which can be used to classify and identify resources. For details, see the tag objects. - Range: None
security_group_rules	Array of SecurityGroupRule objects	- Definition: Security group rule list. - Range: None

Table 5-54 ResponseTag

Parameter	Type	Description
key	String	Definition: Tag key. Range: - A tag key can contain a maximum of 128 Unicode characters and cannot be left blank. - Each tag key of a resource must be unique. - The value can contain: - Letters - Digits - Special characters: underscores (_), hyphens (-) - Chinese characters
value	String	Definition: Tag value. Range: - Each value can contain a maximum of 255 Unicode characters and can be left blank. - The value can contain: - Letters - Digits - Special characters: underscores (_), hyphens (-), periods (.) - Chinese characters

Table 5-55 SecurityGroupRule

Parameter	Type	Description
id	String	- Definition: ID of a security group rule. After a security group rule is created, a security group rule ID is generated, which uniquely identifies the security group rule. - Range: The value is in UUID format with hyphens (-).
description	String	- Definition: Description of a security group rule. - Range: The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
security_group_id	String	- Definition: ID of the security group that a security group rule belongs to. - Range: None
direction	String	- Definition: Inbound or outbound direction of a security group rule. - Range: – ingress: inbound direction – egress: outbound direction
protocol	String	- Definition: Communication protocol of a security group rule. - Range: – icmp – tcp – udp – icmpv6 – IP protocol number
ethertype	String	- Definition: IP address version of a security group rule. - Range: – IPv4 – IPv6

Parameter	Type	Description
multiport	String	- Definition: Port range of a security group rule. - 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	- Definition: Action of a security group rule. - Range: – allow – deny
priority	Integer	- Definition: Priority of a security group rule. - Range: The value is from 1 to 100. The value 1 indicates the highest priority.
remote_group_id	String	- Definition: ID of the remote security group of a security group rule. If the action of the rule is allow, the traffic from the remote security group is allowed. If the action of the rule is deny, the traffic from the remote security group is denied. - Range: ID of an existing security group.
remote_ip_prefix	String	- Definition: Remote IP address of a security group rule. – If direction is set to egress, the IP address is the outbound destination and will be accessed by instances in the security group. – If direction is set to ingress, the IP address is the inbound source and will access the instances in the security group. - Range: CIDR notation format. If an IP address is transferred in the request, the IP address is automatically formatted with /32 as the subnet mask, for example, 192.168.21.45/32.

Parameter	Type	Description
remote_address_group_id	String	- Definition: ID of the remote IP address group of a security group rule. - Range: ID of an existing IP address group.
created_at	String	- Definition: Time when a security group rule was created. - Range: UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
updated_at	String	- Definition: Time when a security group rule was updated. - Range: UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
project_id	String	- Definition: ID of the project that a security group rule belongs to. - Range: None
enabled	Boolean	- Definition: Whether to enable a security group rule. - Range: true: The security group rule is enabled. false: The security group rule is disabled.

Status code: 202**Table 5-56** Response body parameters

Parameter	Type	Description
request_id	String	- Definition: Request ID. - Range: None
error_msg	String	- Definition: Error message. - Range: None
error_code	String	- Definition: Error code. - Range: None

Example Requests

Change the name of the security group whose ID is 69c999ad-d9ef-4d79-94fd-35e6ceb75325 to **security_group_2** and its description to **modified description**.

```
PUT https://{Endpoint}/v3/{project_id}/vpc/security-groups/69c999ad-d9ef-4d79-94fd-35e6ceb75325

{
  "security_group": {
    "name": "security_group_2",
    "description": "modified description"
  }
}
```

Example Responses

Status code: 200

Normal response to the PUT operation. For more status codes, see [Status Codes](#).

```
• {
  "security_group": {
    "id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
    "name": "security_group_2",
    "project_id": "060576782980d5762f9ec014dd2f1148",
    "description": "modified description",
    "enterprise_project_id": 0,
    "tags": [ ],
    "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",
      "description": "",
      "created_at": "2020-07-09T05:56:27.000+00:00",
      "updated_at": "2020-07-09T05:56:27.000+00:00",
      "ethertype": "IPv6",
      "action": "allow",
      "priority": 100,
      "protocol": null,
      "multiport": null,
      "remote_ip_prefix": null,
      "remote_address_group_id": null,
      "enabled": true
    }, {
      "id": "3d6480e8-9ea4-46dc-bb1b-8db190cd5677",
      "project_id": "060576782980d5762f9ec014dd2f1148",
      "security_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
      "direction": "egress",
      "description": "",
      "created_at": "2020-07-09T05:56:27.000+00:00",
      "updated_at": "2020-07-09T05:56:27.000+00:00",
      "ethertype": "IPv6",
      "action": "allow",
      "priority": 100,
      "protocol": null,
      "multiport": null,
      "remote_ip_prefix": null,
      "remote_group_id": null,
      "remote_address_group_id": null,
      "enabled": true
    }, {
      "id": "9581f18c-1fdd-43da-ace9-7758a56ef28a",
      "project_id": "060576782980d5762f9ec014dd2f1148",
      "security_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
```



```
"direction" : "egress",
"description" : "",
"created_at" : "2020-07-09T05:56:27.000+00:00",
"updated_at" : "2020-07-09T05:56:27.000+00:00",
"ethertype" : "IPv4",
"action" : "allow",
"priority" : 100,
"protocol" : null,
"multiport" : null,
"remote_ip_prefix" : null,
"remote_group_id" : null,
"remote_address_group_id" : null,
"enabled" : true
}, {
  "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",
  "description" : "",
  "created_at" : "2020-07-09T05:56:27.000+00:00",
  "updated_at" : "2020-07-09T05:56:27.000+00:00",
  "ethertype" : "IPv4",
  "action" : "allow",
  "priority" : 100,
  "protocol" : null,
  "multiport" : null,
  "remote_ip_prefix" : null,
  "remote_address_group_id" : null,
  "enabled" : true
} ],
"created_at" : "2020-07-09T05:56:27.000+00:00",
"updated_at" : "2020-07-09T05:56:27.000+00:00"
},
"request_id" : "a8cf4f79ca3c22ca685e7e8872e8c20b"
}
```

Status code: 202

Normal response for the specified pre-check request of API V3. For more status codes, see [Status Code](#).

```
{
  "error_msg" : "Request validation has been passed with dry run...",
  "error_code" : "SYS.0202",
  "request_id" : "cfd81aea3f59eac7128dba4b36d516c8"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Change the name of the security group whose ID is 69c999ad-d9ef-4d79-94fd-35e6ceb75325 to **security_group_2** and its description to **modified description**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
```

```
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class UpdateSecurityGroupSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();
        UpdateSecurityGroupRequest request = new UpdateSecurityGroupRequest();
        request.withSecurityGroupId("{security_group_id}");
        UpdateSecurityGroupRequestBody body = new UpdateSecurityGroupRequestBody();
        UpdateSecurityGroupOption securityGroupbody = new UpdateSecurityGroupOption();
        securityGroupbody.withName("security_group_2")
            .withDescription("modified description");
        body.withSecurityGroup(securityGroupbody);
        request.withBody(body);
        try {
            UpdateSecurityGroupResponse response = client.updateSecurityGroup(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrMsg());
        }
    }
}
```

Python

Change the name of the security group whose ID is 69c999ad-d9ef-4d79-94fd-35e6ceb75325 to **security_group_2** and its description to **modified description**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
```

```
# In this example, AK and SK are stored in environment variables for authentication. Before running this
example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak = os.environ["CLOUD_SDK_AK"]
sk = os.environ["CLOUD_SDK_SK"]
projectId = "{project_id}"

credentials = BasicCredentials(ak, sk, projectId)

client = VpcClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(VpcRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = UpdateSecurityGroupRequest()
    request.security_group_id = "{security_group_id}"
    securityGroupbody = UpdateSecurityGroupOption(
        name="security_group_2",
        description="modified description"
    )
    request.body = UpdateSecurityGroupRequestBody(
        security_group=securityGroupbody
    )
    response = client.update_security_group(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

Change the name of the security group whose ID is 69c999ad-d9ef-4d79-94fd-35e6ceb75325 to **security_group_2** and its description to **modified description**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())
```

```
request := &model.UpdateSecurityGroupRequest{
    request.SecurityGroupId = "{security_group_id}"
    nameSecurityGroup:= "security_group_2"
    descriptionSecurityGroup:= "modified description"
    securityGroupbody := &model.UpdateSecurityGroupOption{
        Name: &nameSecurityGroup,
        Description: &descriptionSecurityGroup,
    }
    request.Body = &model.UpdateSecurityGroupRequestBody{
        SecurityGroup: securityGroupbody,
    }
    response, err := client.UpdateSecurityGroup(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Normal response to the PUT operation. For more status codes, see Status Codes .
202	Normal response for the specified pre-check request of API V3. For more status codes, see Status Code .

Error Codes

See [Error Codes](#).

5.2.5 Deleting a Security Group

Function

You can call this API to delete a security group that is no longer used.

Constraints

Before deleting a security group, ensure that the security group is not associated with any instance.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v3/{project_id}/vpc/security-groups/{security_group_id}

Table 5-57 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	- Definition: ID of the project that a security group belongs to. For details about how to obtain a project ID, see Obtaining a Project ID. - Range: None
security_group_id	Yes	String	- Definition: ID of a security group. - Range: None

Request Parameters

None

Response Parameters

Status code: 204

Normal response to the DELETE operation. For more status codes, see [Status Codes](#).

None

Example Requests

Deleting a security group

```
DELETE https://{Endpoint}/v3/{project_id}/vpc/security-groups/69c999ad-d9ef-4d79-94fd-35e6ceb75325
```

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
```

```
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class DeleteSecurityGroupSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();
        DeleteSecurityGroupRequest request = new DeleteSecurityGroupRequest();
        request.withSecurityGroupId("{security_group_id}");
        try {
            DeleteSecurityGroupResponse response = client.deleteSecurityGroup(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)
```

```
client = VpcClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(VpcRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = DeleteSecurityGroupRequest()
    request.security_group_id = "{security_group_id}"
    response = client.delete_security_group(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteSecurityGroupRequest{}
    request.SecurityGroupId = "{security_group_id}"
    response, err := client.DeleteSecurityGroup(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
204	Normal response to the DELETE operation. For more status codes, see Status Codes .

Error Codes

See [Error Codes](#).

5.3 Security Group Rule

5.3.1 Creating a Security Group Rule

Function

A security group has inbound and outbound rules to control traffic that is allowed to reach or leave the instances associated with the security group.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v3/{project_id}/vpc/security-group-rules

Table 5-58 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	- Definition: ID of the project that a security group rule belongs to. For details about how to obtain a project ID, see Obtaining a Project ID. - Range: None

Request Parameters

Table 5-59 Request body parameters

Parameter	Mandatory	Type	Description
dry_run	No	Boolean	• Definition: Whether to only send the check request. • Constraints: None • Range: – true: A check request will be sent and no security group rule will be created. Check items include mandatory parameters, request format, and constraints. If the check fails, an error will be returned. If the check succeeds, response code 202 will be returned. – false: A request will be sent and a security group rule will be created. • Default Value: false
security_group_rule	Yes	CreateSecurityGroupRuleOption object	• Definition: Request body for creating a security group rule. • Constraints: None • Range: None • Default Value: None

Table 5-60 CreateSecurityGroupRuleOption

Parameter	Mandatory	Type	Description
security_group_id	Yes	String	• Definition: ID of the security group that a security group rule belongs to. • Constraints: None • Range: None • Default Value: None

Parameter	Mandatory	Type	Description
description	No	String	• Definition: Description of a security group rule. • Constraints: The value can contain no more than 255 characters and cannot contain angle brackets (< or >). • Range: None • Default Value: None
direction	Yes	String	• Definition: Inbound or outbound direction of a security group rule. • Constraints: None • Range: – ingress: inbound direction – egress: outbound direction • Default Value: None
ethertype	No	String	• Definition: IP address version of a security group rule. • Constraints: None • Range: – IPv4 – IPv6 • Default Value: IPv4

Parameter	Mandatory	Type	Description
protocol	No	String	• Definition: Communication protocol of a security group rule. • Constraints: – If the parameter is left blank, all protocols are supported. – If the protocol is icmpv6, IP version should be IPv6. – If the protocol is icmp, IP version should be IPv4. • Range: – icmp – tcp – udp – icmpv6 – IP protocol number (0-255) • Default Value: None
multiport	No	String	• Definition: Port range of a security group rule. • Constraints: The port number ranges from 1 to 65535. • Range: The value can be a single port (80), a port range (1-30), or inconsecutive ports separated by commas (22,3389,80). • Default Value: None

Parameter	Mandatory	Type	Description
remote_ip_prefix	No	String	• Definition: Remote IP address of a security group rule. If direction is set to egress, this address is the outbound destination and will be accessed by instances in the security group. If direction is set to ingress, this address is the inbound source and will access instances in the security group. • Constraints: – This parameter is mutually exclusive with parameters remote_group_id and remote_address_group_id. – If this parameter is left blank, traffic from all remote IP addresses is allowed when the action of the rule is allow, and is denied when the action of the rule is deny. • Range: – IP address. If an IP address is specified in the request, the IP address is automatically formatted with /32 as the subnet mask, for example, 192.168.21.45/32. – The value must be in CIDR format. • Default Value: None

Parameter	Mandatory	Type	Description
remote_group_id	No	String	• Definition: ID of the remote security group of a security group rule. If the action of the rule is allow, the traffic from the remote security group is allowed. If the action of the rule is deny, the traffic from the remote security group is denied. • Constraints: The parameter is mutually exclusive with parameters remote_ip_prefix and remote_address_group_id. • Range: ID of an existing security group. • Default Value: None
remote_address_group_id	No	String	• Definition: ID of the remote IP address group of a security group rule. • Constraints: The parameter is mutually exclusive with parameters remote_ip_prefix and remote_group_id. • Range: ID of an existing IP address group. • Default Value: None
action	No	String	• Definition: Action of a security group rule. • Constraints: None • Range: – allow – deny • Default Value: allow
priority	No	String	• Definition: Priority of a security group rule. • Constraints: None • Range: The value is from 1 to 100. The value 1 indicates the highest priority. • Default Value: 1

Parameter	Mandatory	Type	Description
enabled	No	Boolean	• Definition: Whether to enable a security group rule. • Constraints: None • Range: – true: The security group rule is enabled. – false: The security group rule is disabled. • Default Value: true

Response Parameters

Status code: 201

Table 5-61 Response body parameters

Parameter	Type	Description
request_id	String	• Definition: Request ID. • Range: None
security_group_rule	SecurityGroupRule object	• Definition: Response body for creating a security group rule. • Range: None

Table 5-62 SecurityGroupRule

Parameter	Type	Description
id	String	• Definition: ID of a security group rule. After a security group rule is created, a security group rule ID is generated, which uniquely identifies the security group rule. • Range: The value is in UUID format with hyphens (-).
description	String	• Definition: Description of a security group rule. • Range: The value can contain no more than 255 characters and cannot contain angle brackets (< or >).

Parameter	Type	Description
security_group_id	String	- Definition: ID of the security group that a security group rule belongs to. - Range: None
direction	String	- Definition: Inbound or outbound direction of a security group rule. - Range: ingress: inbound direction egress: outbound direction
protocol	String	- Definition: Communication protocol of a security group rule. - Range: icmp tcp udp icmpv6 - IP protocol number
ethertype	String	- Definition: IP address version of a security group rule. - Range: - IPv4 - IPv6
multiport	String	- Definition: Port range of a security group rule. - 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	- Definition: Action of a security group rule. - Range: allow deny
priority	Integer	- Definition: Priority of a security group rule. - Range: The value is from 1 to 100. The value 1 indicates the highest priority.

Parameter	Type	Description
remote_group_id	String	- Definition: ID of the remote security group of a security group rule. If the action of the rule is allow, the traffic from the remote security group is allowed. If the action of the rule is deny, the traffic from the remote security group is denied. - Range: ID of an existing security group.
remote_ip_prefix	String	- Definition: Remote IP address of a security group rule. - If direction is set to egress, the IP address is the outbound destination and will be accessed by instances in the security group. - If direction is set to ingress, the IP address is the inbound source and will access the instances in the security group. - Range: CIDR notation format. If an IP address is transferred in the request, the IP address is automatically formatted with /32 as the subnet mask, for example, 192.168.21.45/32.
remote_address_group_id	String	- Definition: ID of the remote IP address group of a security group rule. - Range: ID of an existing IP address group.
created_at	String	- Definition: Time when a security group rule was created. - Range: UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
updated_at	String	- Definition: Time when a security group rule was updated. - Range: UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
project_id	String	- Definition: ID of the project that a security group rule belongs to. - Range: None

Parameter	Type	Description
enabled	Boolean	- Definition: Whether to enable a security group rule. - Range: true: The security group rule is enabled. false: The security group rule is disabled.

Status code: 202

Table 5-63 Response body parameters

Parameter	Type	Description
request_id	String	- Definition: Request ID. - Range: None
error_msg	String	- Definition: Error message. - Range: None
error_code	String	- Definition: Error code. - Range: None

Example Requests

Create an inbound rule in the security group whose ID is 0552091e-b83a-49dd-88a7-4a5c86fd9ec3.

POST https://{Endpoint}/v3/{project_id}/vpc/security-group-rules

```
{
  "security_group_rule": {
    "security_group_id": "0552091e-b83a-49dd-88a7-4a5c86fd9ec3",
    "direction": "ingress",
    "protocol": "tcp",
    "description": "security group rule description",
    "action": "allow",
    "priority": 1,
    "multiport": "33",
    "remote_ip_prefix": "10.10.0.0/16"
  }
}
```

Example Responses

Status code: 201

Normal response to the POST operation. For more status codes, see [Status Codes](#).

- ```
{
 "request_id": "1666b2708aaf849337572d6846dce781",
```

```
"security_group_rule" : {
 "id" : "f626eb24-d8bd-4d26-ae0b-c16bb65730cb",
 "project_id" : "060576782980d5762f9ec014dd2f1148",
 "security_group_id" : "0552091e-b83a-49dd-88a7-4a5c86fd9ec3",
 "direction" : "ingress",
 "protocol" : "tcp",
 "description" : "security group rule description",
 "created_at" : "2020-08-13T07:12:36.000+00:00",
 "updated_at" : "2020-08-13T07:12:36.000+00:00",
 "ethertype" : "IPv4",
 "remote_ip_prefix" : "10.10.0.0/16",
 "multiport" : 33,
 "action" : "allow",
 "priority" : 1,
 "remote_group_id" : null,
 "remote_address_group_id" : null,
 "enabled" : true
}
```

**Status code: 202**

Normal response for the specified pre-check request of API V3. For more status codes, see [Status Code](#).

```
{
 "error_msg" : "Request validation has been passed with dry run...",
 "error_code" : "SYS.0202",
 "request_id" : "cfd81aea3f59eac7128dba4b36d516c8"
}
```

## SDK Sample Code

The SDK sample code is as follows.

### Java

Create an inbound rule in the security group whose ID is 0552091e-b83a-49dd-88a7-4a5c86fd9ec3.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class CreateSecurityGroupRuleSolution {

 public static void main(String[] args) {
 // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
 // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
 // environment variables and decrypted during use to ensure security.
 // In this example, AK and SK are stored in environment variables for authentication. Before running
 // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
 String ak = System.getenv("CLOUD_SDK_AK");
 String sk = System.getenv("CLOUD_SDK_SK");
 String projectId = "{project_id}";

 ICredential auth = new BasicCredentials()
 .withProjectId(projectId)
 .withAk(ak)
```

```
.withSk(sk);

VpcClient client = VpcClient.newBuilder()
 .withCredential(auth)
 .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
 .build();
CreateSecurityGroupRuleRequest request = new CreateSecurityGroupRuleRequest();
CreateSecurityGroupRuleRequestBody body = new CreateSecurityGroupRuleRequestBody();
CreateSecurityGroupRuleOption securityGroupRuleOption = new CreateSecurityGroupRuleOption();
securityGroupRulebody.withSecurityGroupId("0552091e-b83a-49dd-88a7-4a5c86fd9ec3")
 .withDescription("security group rule description")
 .withDirection("ingress")
 .withProtocol("tcp")
 .withMultiport("33")
 .withRemoteIpPrefix("10.10.0.0/16")
 .withAction("allow")
 .withPriority("1");
body.withSecurityGroupRule(securityGroupRulebody);
request.withBody(body);
try {
 CreateSecurityGroupRuleResponse response = client.createSecurityGroupRule(request);
 System.out.println(response.toString());
} catch (ConnectionException e) {
 e.printStackTrace();
} catch (RequestTimeoutException e) {
 e.printStackTrace();
} catch (ServiceResponseException e) {
 e.printStackTrace();
 System.out.println(e.getStatusCode());
 System.out.println(e.getRequestId());
 System.out.println(e.getErrorCode());
 System.out.println(e.getErrorMsg());
}
}
```

## Python

Create an inbound rule in the security group whose ID is 0552091e-b83a-49dd-88a7-4a5c86fd9ec3.

```
coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
 # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
 # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
 # variables and decrypted during use to ensure security.
 # In this example, AK and SK are stored in environment variables for authentication. Before running this
 # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
 ak = os.environ["CLOUD_SDK_AK"]
 sk = os.environ["CLOUD_SDK_SK"]
 projectId = "{project_id}"

 credentials = BasicCredentials(ak, sk, projectId)

 client = VpcClient.new_builder() \
 .with_credentials(credentials) \
 .with_region(VpcRegion.value_of("<YOUR REGION>")) \
 .build()

 try:
 request = CreateSecurityGroupRuleRequest()
 securityGroupRulebody = CreateSecurityGroupRuleOption(
```

```
 security_group_id="0552091e-b83a-49dd-88a7-4a5c86fd9ec3",
 description="security group rule description",
 direction="ingress",
 protocol="tcp",
 multiport="33",
 remote_ip_prefix="10.10.0.0/16",
 action="allow",
 priority="1"
)
 request.body = CreateSecurityGroupRuleRequestBody(
 security_group_rule=securityGroupRulebody
)
 response = client.create_security_group_rule(request)
 print(response)
except exceptions.ClientRequestException as e:
 print(e.status_code)
 print(e.request_id)
 print(e.error_code)
 print(e.error_msg)
```

## Go

Create an inbound rule in the security group whose ID is 0552091e-b83a-49dd-88a7-4a5c86fd9ec3.

```
package main

import (
 "fmt"
 "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
 vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
 "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
 region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
 // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
 // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
 // variables and decrypted during use to ensure security.
 // In this example, AK and SK are stored in environment variables for authentication. Before running this
 // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
 ak := os.Getenv("CLOUD_SDK_AK")
 sk := os.Getenv("CLOUD_SDK_SK")
 projectId := "{project_id}"

 auth := basic.NewCredentialsBuilder().
 WithAk(ak).
 WithSk(sk).
 WithProjectId(projectId).
 Build()

 client := vpc.NewVpcClient(
 vpc.VpcClientBuilder().
 WithRegion(region.ValueOf("<YOUR REGION>")).
 WithCredential(auth).
 Build())

 request := &model.CreateSecurityGroupRuleRequest{
 descriptionSecurityGroupRule: "security group rule description"
 protocolSecurityGroupRule: "tcp"
 multiportSecurityGroupRule: "33"
 remoteIpPrefixSecurityGroupRule: "10.10.0.0/16"
 actionSecurityGroupRule: "allow"
 prioritySecurityGroupRule: "1"
 securityGroupRulebody := &model.CreateSecurityGroupRuleOption{
 SecurityGroupId: "0552091e-b83a-49dd-88a7-4a5c86fd9ec3",
 Description: &descriptionSecurityGroupRule,
 Direction: "ingress",
 Protocol: &protocolSecurityGroupRule,
```

```
Multiport: &multiportSecurityGroupRule,
RemotelyPrefix: &remotelyPrefixSecurityGroupRule,
Action: &actionSecurityGroupRule,
Priority: &prioritySecurityGroupRule,
}
request.Body = &model.CreateSecurityGroupRuleRequestBody{
 SecurityGroupRule: securityGroupRulebody,
}
response, err := client.CreateSecurityGroupRule(request)
if err == nil {
 fmt.Printf("%v\n", response)
} else {
 fmt.Println(err)
}
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

| Status Code | Description                                                                                                             |
|-------------|-------------------------------------------------------------------------------------------------------------------------|
| 201         | Normal response to the POST operation. For more status codes, see <a href="#">Status Codes</a> .                        |
| 202         | Normal response for the specified pre-check request of API V3. For more status codes, see <a href="#">Status Code</a> . |

Error Codes

See [Error Codes](#).

5.3.2 Querying a Security Group Rule

Function

After a security group rule is created, you can call this API to query all information about the security group rule, including the ID and protocol.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v3/{project\_id}/vpc/security-group-rules/{security\_group\_rule\_id}

Table 5-64 Path Parameters

| Parameter              | Mandatory | Type   | Description                                                                                                                                                                                                                                                                                          |
|------------------------|-----------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| project_id             | Yes       | String | <ul style="list-style-type: none"><li>Definition: ID of the project that a security group rule belongs to. For details about how to obtain a project ID, see <a href="#">Obtaining a Project ID</a>.</li><li>Range: None</li></ul>                                                                   |
| security_group_rule_id | Yes       | String | <ul style="list-style-type: none"><li>Definition: Security group rule ID. You can call the API <a href="#">Querying Security Group Rules</a> to obtain the ID of the target security group rule, and then use this API to query details about the security group rule.</li><li>Range: None</li></ul> |

Request Parameters

None

Response Parameters

Status code: 200

Table 5-65 Response body parameters

| Parameter           | Type                                     | Description                                                                                                                                     |
|---------------------|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| request_id          | String                                   | <ul style="list-style-type: none"><li>Definition: Request ID.</li><li>Range: None</li></ul>                                                     |
| security_group_rule | <a href="#">SecurityGroupRule</a> object | <ul style="list-style-type: none"><li>Definition: Response body for querying details about a security group rule.</li><li>Range: None</li></ul> |

**Table 5-66** SecurityGroupRule

| Parameter         | Type   | Description                                                                                                                                                                                                                                                                             |
|-------------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| id                | String | <ul style="list-style-type: none"><li>Definition: ID of a security group rule. After a security group rule is created, a security group rule ID is generated, which uniquely identifies the security group rule.</li><li>Range: The value is in UUID format with hyphens (-).</li></ul> |
| description       | String | <ul style="list-style-type: none"><li>Definition: Description of a security group rule.</li><li>Range: The value can contain no more than 255 characters and cannot contain angle brackets (&lt; or &gt;).</li></ul>                                                                    |
| security_group_id | String | <ul style="list-style-type: none"><li>Definition: ID of the security group that a security group rule belongs to.</li><li>Range: None</li></ul>                                                                                                                                         |
| direction         | String | <ul style="list-style-type: none"><li>Definition: Inbound or outbound direction of a security group rule.</li><li>Range:<ul style="list-style-type: none"><li>– <b>ingress</b>: inbound direction</li><li>– <b>egress</b>: outbound direction</li></ul></li></ul>                       |
| protocol          | String | <ul style="list-style-type: none"><li>Definition: Communication protocol of a security group rule.</li><li>Range:<ul style="list-style-type: none"><li>– <b>icmp</b></li><li>– <b>tcp</b></li><li>– <b>udp</b></li><li>– <b>icmpv6</b></li><li>– IP protocol number</li></ul></li></ul> |
| ethertype         | String | <ul style="list-style-type: none"><li>Definition: IP address version of a security group rule.</li><li>Range:<ul style="list-style-type: none"><li>– IPv4</li><li>– IPv6</li></ul></li></ul>                                                                                            |

| Parameter        | Type    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| multiport        | String  | <ul style="list-style-type: none"><li>Definition: Port range of a security group rule.</li><li>Range: The value can be a single port (80), a port range (1-30), or inconsecutive ports separated by commas (22,3389,80).</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                     |
| action           | String  | <ul style="list-style-type: none"><li>Definition: Action of a security group rule.</li><li>Range:<ul style="list-style-type: none"><li>– <b>allow</b></li><li>– <b>deny</b></li></ul></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| priority         | Integer | <ul style="list-style-type: none"><li>Definition: Priority of a security group rule.</li><li>Range: The value is from 1 to 100. The value 1 indicates the highest priority.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| remote_group_id  | String  | <ul style="list-style-type: none"><li>Definition: ID of the remote security group of a security group rule. If the action of the rule is <b>allow</b>, the traffic from the remote security group is allowed. If the action of the rule is <b>deny</b>, the traffic from the remote security group is denied.</li><li>Range: ID of an existing security group.</li></ul>                                                                                                                                                                                                                                                                               |
| remote_ip_prefix | String  | <ul style="list-style-type: none"><li>Definition: Remote IP address of a security group rule.<ul style="list-style-type: none"><li>– If <b>direction</b> is set to <b>egress</b>, the IP address is the outbound destination and will be accessed by instances in the security group.</li><li>– If <b>direction</b> is set to <b>ingress</b>, the IP address is the inbound source and will access the instances in the security group.</li></ul></li><li>Range: CIDR notation format. If an IP address is transferred in the request, the IP address is automatically formatted with /32 as the subnet mask, for example, 192.168.21.45/32.</li></ul> |



| Parameter               | Type    | Description                                                                                                                                                                                                                                                                    |
|-------------------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| remote_address_group_id | String  | <ul style="list-style-type: none"><li>Definition: ID of the remote IP address group of a security group rule.</li><li>Range: ID of an existing IP address group.</li></ul>                                                                                                     |
| created_at              | String  | <ul style="list-style-type: none"><li>Definition: Time when a security group rule was created.</li><li>Range: UTC time in the format of yyyy-MM-ddTHH:mm:ssZ</li></ul>                                                                                                         |
| updated_at              | String  | <ul style="list-style-type: none"><li>Definition: Time when a security group rule was updated.</li><li>Range: UTC time in the format of yyyy-MM-ddTHH:mm:ssZ</li></ul>                                                                                                         |
| project_id              | String  | <ul style="list-style-type: none"><li>Definition: ID of the project that a security group rule belongs to.</li><li>Range: None</li></ul>                                                                                                                                       |
| enabled                 | Boolean | <ul style="list-style-type: none"><li>Definition: Whether to enable a security group rule.</li><li>Range:<ul style="list-style-type: none"><li><b>true</b>: The security group rule is enabled.</li><li><b>false</b>: The security group rule is disabled.</li></ul></li></ul> |

## Example Requests

Query details about a security group rule.

GET https://{Endpoint}/v3/{project\_id}/vpc/security-group-rules/f626eb24-d8bd-4d26-ae0b-c16bb65730cb

## Example Responses

**Status code: 200**

Normal response to the GET operation. For more status codes, see [Status Codes](#).

- ```
{
  "security_group_rule": {
    "id": "f626eb24-d8bd-4d26-ae0b-c16bb65730cb",
    "project_id": "060576782980d5762f9ec014dd2f1148",
    "security_group_id": "0552091e-b83a-49dd-88a7-4a5c86fd9ec3",
    "direction": "ingress",
    "protocol": "tcp",
    "description": "security group rule description",
    "created_at": "2020-08-13T07:12:36.000+00:00",
    "updated_at": "2020-08-13T07:12:36.000+00:00",
    "ethertype": "IPv4",
    "remote_ip_prefix": "10.10.0.0/16",
    "multiport": 333,
  }
}
```

```
"action" : "allow",
"priority" : 1,
"remote_group_id" : null,
"remote_address_group_id" : null,
"enabled" : true
},
"request_id" : "034c4840bde0b1263a4b2e66fbd74d5f"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class ShowSecurityGroupRuleSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();
        ShowSecurityGroupRuleRequest request = new ShowSecurityGroupRuleRequest();
        request.withSecurityGroupId("{security_group_id}");
        try {
            ShowSecurityGroupRuleResponse response = client.showSecurityGroupRule(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowSecurityGroupRuleRequest()
        request.security_group_rule_id = "{security_group_rule_id}"
        response = client.show_security_group_rule(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
```

```
WithCredential(auth).  
Build())  
  
request := &model.ShowSecurityGroupRuleRequest{}  
request.SecurityGroupRuleId = "{security_group_rule_id}"  
response, err := client.ShowSecurityGroupRule(request)  
if err == nil {  
    fmt.Printf("%v\n", response)  
} else {  
    fmt.Println(err)  
}  
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Normal response to the GET operation. For more status codes, see Status Codes .

Error Codes

See [Error Codes](#).

5.3.3 Querying Security Group Rules

Function

After a security group rule is created, you can call this API to query all information about the security group rule, including the ID and protocol.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v3/{project_id}/vpc/security-group-rules

Table 5-67 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	- Definition: Project ID. For details about how to obtain a project ID, see Obtaining a Project ID. - Range: None

Table 5-68 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	- Definition: Number of records returned on each page. - Range: 0-2000
marker	No	String	- Definition: ID of the resource from which the pagination query starts. If the parameter is left blank, only resources on the first page are queried. - Range: Security group rule ID.
id	No	Array of strings	- Definition: ID of a security group rule. Multiple IDs can be specified for filtering. - Range: None
security_group_id	No	Array of strings	- Definition: ID of the security group that a security group rule belongs to. Multiple IDs can be specified for filtering. - Range: None
protocol	No	Array of strings	- Definition: Communication protocol of a security group rule. Multiple values can be specified for filtering. - Range: None
description	No	Array of strings	- Definition: Description of a security group rule. Multiple descriptions can be specified for filtering. - Range: None

Parameter	Mandatory	Type	Description
remote_group_id	No	Array of strings	• Definition: Remote security group ID of a security group rule. Multiple IDs can be specified for filtering. • Range: None
direction	No	String	• Definition: Inbound or outbound direction of a security group rule. • Range: – ingress: inbound direction – egress: outbound direction
action	No	String	• Definition: Action of a security group rule. • Range: – allow – deny
remote_ip_prefix	No	String	• Definition: Remote IP address of a security group rule. • Range: The value must be in CIDR format.
enabled	No	Boolean	• Definition: Whether a security group rule is enabled. Only one value can be specified for filtering. • Range: – true: The enabled security group rule is filtered. – false: The disabled security group rule is filtered.
priority	No	Array of integers	• Definition: Priority of a security group rule. Multiple values can be specified for filtering. • Range: None

Parameter	Mandatory	Type	Description
ethertype	No	Array of strings	- Definition: IP address version of a security group rule. Multiple values can be specified for filtering. - Range: IPv4, IPv6, ipv4, and ipv6
remote_address_group_id	No	Array of strings	- Definition: Remote IP address group ID of a security group rule. Multiple IDs can be specified for filtering. - Range: None

Request Parameters

None

Response Parameters

Status code: 200

Table 5-69 Response body parameters

Parameter	Type	Description
request_id	String	- Definition: Request ID. - Range: None
security_group_rules	Array of SecurityGroupRule objects	- Definition: Response body for querying security group rules. - Range: None
page_info	PageInfo object	- Definition: Pagination information. - Range: None

Table 5-70 SecurityGroupRule

Parameter	Type	Description
id	String	- Definition: ID of a security group rule. After a security group rule is created, a security group rule ID is generated, which uniquely identifies the security group rule. - Range: The value is in UUID format with hyphens (-).
description	String	- Definition: Description of a security group rule. - Range: The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
security_group_id	String	- Definition: ID of the security group that a security group rule belongs to. - Range: None
direction	String	- Definition: Inbound or outbound direction of a security group rule. - Range: – ingress: inbound direction – egress: outbound direction
protocol	String	- Definition: Communication protocol of a security group rule. - Range: – icmp – tcp – udp – icmpv6 – IP protocol number
ethertype	String	- Definition: IP address version of a security group rule. - Range: – IPv4 – IPv6

Parameter	Type	Description
multiport	String	- Definition: Port range of a security group rule. - 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	- Definition: Action of a security group rule. - Range: – allow – deny
priority	Integer	- Definition: Priority of a security group rule. - Range: The value is from 1 to 100. The value 1 indicates the highest priority.
remote_group_id	String	- Definition: ID of the remote security group of a security group rule. If the action of the rule is allow, the traffic from the remote security group is allowed. If the action of the rule is deny, the traffic from the remote security group is denied. - Range: ID of an existing security group.
remote_ip_prefix	String	- Definition: Remote IP address of a security group rule. – If direction is set to egress, the IP address is the outbound destination and will be accessed by instances in the security group. – If direction is set to ingress, the IP address is the inbound source and will access the instances in the security group. - Range: CIDR notation format. If an IP address is transferred in the request, the IP address is automatically formatted with /32 as the subnet mask, for example, 192.168.21.45/32.

Parameter	Type	Description
remote_address_group_id	String	- Definition: ID of the remote IP address group of a security group rule. - Range: ID of an existing IP address group.
created_at	String	- Definition: Time when a security group rule was created. - Range: UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
updated_at	String	- Definition: Time when a security group rule was updated. - Range: UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
project_id	String	- Definition: ID of the project that a security group rule belongs to. - Range: None
enabled	Boolean	- Definition: Whether to enable a security group rule. - Range: true: The security group rule is enabled. false: The security group rule is disabled.

Table 5-71 PageInfo

Parameter	Type	Description
previous_marker	String	Definition: The first record on the current page. Range: N/A
current_count	Integer	Definition: Total number of resources on the current page. Range: N/A

Parameter	Type	Description
next_marker	String	Definition: The last record on the current page. The next_marker field does not exist if the page is the last one. Range: N/A

Example Requests

Query security group rules.

GET https://{Endpoint}/v3/{project_id}/vpc/security-group-rules

Example Responses

Status code: 200

Normal response to the GET operation. For more status codes, see [Status Codes](#).

```
{
  "request_id": "80747d36e3376c0894ba8f9a9156355d",
  "security_group_rules": [ {
    "id": "f626eb24-d8bd-4d26-ae0b-c16bb65730cb",
    "project_id": "060576782980d5762f9ec014dd2f1148",
    "security_group_id": "0552091e-b83a-49dd-88a7-4a5c86fd9ec3",
    "direction": "ingress",
    "protocol": "tcp",
    "description": "security group rule description",
    "created_at": "2020-08-13T07:12:36.000+00:00",
    "updated_at": "2020-08-13T07:12:36.000+00:00",
    "ethertype": "IPv4",
    "remote_ip_prefix": "10.10.0.0/16",
    "multiport": 333,
    "action": "allow",
    "priority": 1,
    "remote_group_id": null,
    "remote_address_group_id": null,
    "enabled": true
  } ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;
```

```
public class ListSecurityGroupRulesSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();
        ListSecurityGroupRulesRequest request = new ListSecurityGroupRulesRequest();
        try {
            ListSecurityGroupRulesResponse response = client.listSecurityGroupRules(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
```

```
request = ListSecurityGroupRulesRequest()
response = client.list_security_group_rules(request)
print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListSecurityGroupRulesRequest{}
    response, err := client.ListSecurityGroupRules(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Normal response to the GET operation. For more status codes, see Status Codes .

Error Codes

See [Error Codes](#).

5.3.4 Deleting a Security Group Rule

Function

You can call this API to delete a security group rule that is no longer used.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v3/{project_id}/vpc/security-group-rules/{security_group_rule_id}

Table 5-72 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	- Definition: Project ID. For details about how to obtain a project ID, see Obtaining a Project ID. - Range: None
security_group_rule_id	Yes	String	- Definition: ID of a security group rule. You can call the API Querying Security Group Rules to obtain the ID of the target security group rule, and then use this API to delete the security group rule. - Range: None

Request Parameters

None

Response Parameters

Status code: 204

Normal response to the DELETE operation. For more status codes, see [Status Codes](#).

None

Example Requests

Delete the security group rule whose ID is f626eb24-d8bd-4d26-ae0b-c16bb65730cb.

```
DELETE https://{Endpoint}/v3/{project_id}/vpc/security-group-rules/f626eb24-d8bd-4d26-ae0b-c16bb65730cb
```

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class DeleteSecurityGroupRuleSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();
        DeleteSecurityGroupRuleRequest request = new DeleteSecurityGroupRuleRequest();
        request.withSecurityGroupRuleId("{security_group_rule_id}");
        try {
            DeleteSecurityGroupRuleResponse response = client.deleteSecurityGroupRule(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

```
}  
}  
}
```

Python

```
# coding: utf-8  
  
import os  
from huaweicloudsdkcore.auth.credentials import BasicCredentials  
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion  
from huaweicloudsdkcore.exceptions import exceptions  
from huaweicloudsdkvpc.v3 import *  
  
if __name__ == "__main__":  
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security  
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment  
    # variables and decrypted during use to ensure security.  
    # In this example, AK and SK are stored in environment variables for authentication. Before running this  
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak = os.environ["CLOUD_SDK_AK"]  
    sk = os.environ["CLOUD_SDK_SK"]  
    projectId = "{project_id}"  
  
    credentials = BasicCredentials(ak, sk, projectId)  
  
    client = VpcClient.new_builder() \  
        .with_credentials(credentials) \  
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \  
        .build()  
  
    try:  
        request = DeleteSecurityGroupRuleRequest()  
        request.security_group_rule_id = "{security_group_rule_id}"  
        response = client.delete_security_group_rule(request)  
        print(response)  
    except exceptions.ClientRequestException as e:  
        print(e.status_code)  
        print(e.request_id)  
        print(e.error_code)  
        print(e.error_msg)
```

Go

```
package main  
  
import (  
    "fmt"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"  
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"  
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"  
)  
  
func main() {  
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security  
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment  
    // variables and decrypted during use to ensure security.  
    // In this example, AK and SK are stored in environment variables for authentication. Before running this  
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak := os.Getenv("CLOUD_SDK_AK")  
    sk := os.Getenv("CLOUD_SDK_SK")  
    projectId := "{project_id}"  
  
    auth := basic.NewCredentialsBuilder().  
        WithAk(ak).  
        WithSk(sk).  
        WithProjectId(projectId).  
        Build()
```



```
client := vpc.NewVpcClient(  
    vpc.VpcClientBuilder().  
        WithRegion(region.ValueOf("<YOUR REGION>")).  
        WithCredential(auth).  
        Build())  
  
request := &model.DeleteSecurityGroupRuleRequest{  
    request.SecurityGroupId = "{security_group_id}"  
    response, err := client.DeleteSecurityGroupRule(request)  
    if err == nil {  
        fmt.Printf("%+v\n", response)  
    } else {  
        fmt.Println(err)  
    }  
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
204	Normal response to the DELETE operation. For more status codes, see Status Codes .

Error Codes

See [Error Codes](#).

5.3.5 Adding Rules to a Specified Security Group

Function

You can call the API for creating security group rules in batches in a security group.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v3/{project_id}/vpc/security-groups/{security_group_id}/security-group-rules/batch-create

Table 5-73 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	- Definition: Project ID. For details about how to obtain a project ID, see Obtaining a Project ID. - Range: None
security_group_id	Yes	String	- Definition: ID of a security group. - Range: None

Request Parameters

Table 5-74 Request body parameters

Parameter	Mandatory	Type	Description
security_group_rules	Yes	Array of BatchCreateSecurityGroupRulesOption objects	- Definition: Request body for creating security group rules in batches. - Constraints: A maximum of 200 rules can be specified. - Range: None - Default Value: None

Parameter	Mandatory	Type	Description
ignore_duplicate	No	Boolean	• Definition: Whether to ignore duplicate security group rules during creation. • Constraints: None • Range: – true: Duplicate rules will be ignored. If the request contains duplicate rules or rules same as existing ones in the security group, no error is reported and duplicate rules are not created. – false: Duplicate rules will not be ignored. If the request contains duplicate rules or rules same as existing ones in the security group, an error is reported. • Default Value: false
dry_run	No	Boolean	• Definition: Whether to only send the check request. • Constraints: None • Range: – true: A check request will be sent and no security group rule will be created. Check items include mandatory parameters, request format, and constraints. If the check fails, an error will be returned. If the check succeeds, response code 202 will be returned. – false: A request will be sent and a security group rule will be created. • Default Value: false

Table 5-75 BatchCreateSecurityGroupRulesOption

Parameter	Mandatory	Type	Description
description	No	String	• Definition: Description of a security group rule. • Constraints: The value can contain no more than 255 characters and cannot contain angle brackets (< or >). • Range: None • Default Value: None
direction	Yes	String	• Definition: Inbound or outbound direction of a security group rule. • Constraints: None • Range: – ingress: inbound direction – egress: outbound direction • Default Value: None
ethertype	No	String	• Definition: IP address version of a security group rule. • Constraints: None • Range: – IPv4 – IPv6 • Default Value: IPv4

Parameter	Mandatory	Type	Description
protocol	No	String	• Definition: Communication protocol of a security group rule. • Constraints: – If the parameter is left blank, all protocols are supported. – If the protocol is icmpv6, IP version should be IPv6. – If the protocol is icmp, IP version should be IPv4. • Range: – icmp – tcp – udp – icmpv6 – IP protocol number (0-255) • Default Value: None
multiport	No	String	• Definition: Port range of a security group rule. • Constraints: The port number ranges from 1 to 65535. • Range: The value can be a single port (80), a port range (1-30), or inconsecutive ports separated by commas (22,3389,80). • Default Value: None

Parameter	Mandatory	Type	Description
remote_ip_prefix	No	String	• Definition: Remote IP address of a security group rule. If direction is set to egress, this address is the outbound destination and will be accessed by instances in the security group. If direction is set to ingress, this address is the inbound source and will access instances in the security group. • Constraints: – This parameter is mutually exclusive with parameters remote_group_id and remote_address_group_id. – If this parameter is left blank, traffic from all remote IP addresses is allowed when the action of the rule is allow, and is denied when the action of the rule is deny. • Range: – IP address. If an IP address is specified in the request, the IP address is automatically formatted with /32 as the subnet mask, for example, 192.168.21.45/32. – The value must be in CIDR format. • Default Value: None

Parameter	Mandatory	Type	Description
remote_group_id	No	String	• Definition: ID of the remote security group of a security group rule. If the action of the rule is allow, the traffic from the remote security group is allowed. If the action of the rule is deny, the traffic from the remote security group is denied. • Constraints: The parameter is mutually exclusive with parameters remote_ip_prefix and remote_address_group_id. • Range: ID of an existing security group. • Default Value: None
remote_address_group_id	No	String	• Definition: ID of the remote IP address group of a security group rule. • Constraints: The parameter is mutually exclusive with parameters remote_ip_prefix and remote_group_id. • Range: ID of an existing IP address group. • Default Value: None
action	No	String	• Definition: Action of a security group rule. • Constraints: None • Range: – allow – deny • Default Value: allow
priority	No	String	• Definition: Priority of a security group rule. • Constraints: None • Range: The value is from 1 to 100. The value 1 indicates the highest priority. • Default Value: 1

Parameter	Mandatory	Type	Description
enabled	No	Boolean	• Definition: Whether to enable a security group rule. • Constraints: None • Range: – true: The security group rule is enabled. – false: The security group rule is disabled. • Default Value: true

Response Parameters

Status code: 201

Table 5-76 Response body parameters

Parameter	Type	Description
security_group_rules	Array of SecurityGroupRule objects	• Definition: Response body for creating security group rules in batches. • Range: None
request_id	String	• Definition: Request ID. • Range: None

Table 5-77 SecurityGroupRule

Parameter	Type	Description
id	String	• Definition: ID of a security group rule. After a security group rule is created, a security group rule ID is generated, which uniquely identifies the security group rule. • Range: The value is in UUID format with hyphens (-).
description	String	• Definition: Description of a security group rule. • Range: The value can contain no more than 255 characters and cannot contain angle brackets (< or >).

Parameter	Type	Description
security_group_id	String	- Definition: ID of the security group that a security group rule belongs to. - Range: None
direction	String	- Definition: Inbound or outbound direction of a security group rule. - Range: ingress: inbound direction egress: outbound direction
protocol	String	- Definition: Communication protocol of a security group rule. - Range: icmp tcp udp icmpv6 - IP protocol number
ethertype	String	- Definition: IP address version of a security group rule. - Range: - IPv4 - IPv6
multiport	String	- Definition: Port range of a security group rule. - 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	- Definition: Action of a security group rule. - Range: allow deny
priority	Integer	- Definition: Priority of a security group rule. - Range: The value is from 1 to 100. The value 1 indicates the highest priority.

Parameter	Type	Description
remote_group_id	String	- Definition: ID of the remote security group of a security group rule. If the action of the rule is allow, the traffic from the remote security group is allowed. If the action of the rule is deny, the traffic from the remote security group is denied. - Range: ID of an existing security group.
remote_ip_prefix	String	- Definition: Remote IP address of a security group rule. - If direction is set to egress, the IP address is the outbound destination and will be accessed by instances in the security group. - If direction is set to ingress, the IP address is the inbound source and will access the instances in the security group. - Range: CIDR notation format. If an IP address is transferred in the request, the IP address is automatically formatted with /32 as the subnet mask, for example, 192.168.21.45/32.
remote_address_group_id	String	- Definition: ID of the remote IP address group of a security group rule. - Range: ID of an existing IP address group.
created_at	String	- Definition: Time when a security group rule was created. - Range: UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
updated_at	String	- Definition: Time when a security group rule was updated. - Range: UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
project_id	String	- Definition: ID of the project that a security group rule belongs to. - Range: None

Parameter	Type	Description
enabled	Boolean	- Definition: Whether to enable a security group rule. - Range: true: The security group rule is enabled. false: The security group rule is disabled.

Status code: 202

Table 5-78 Response body parameters

Parameter	Type	Description
request_id	String	- Definition: Request ID. - Range: None
error_msg	String	- Definition: Error message. - Range: None
error_code	String	- Definition: Error code. - Range: None

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

Normal response to the POST operation. For more status codes, see [Status Codes](#).

```
• {
  "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,
    "remote_group_id": null,
    "remote_address_group_id": null,
    "enabled": true
  } ],
  "request_id": "f1ae2c6f9e94babf077cd3b3e1570c81"
}
```

Status code: 202

Normal response for the specified pre-check request of API V3. For more status codes, see [Status Code](#).

```
{
  "error_msg": "Request validation has been passed with dry run...",
  "error_code": "SYS.0202",
  "request_id": "cfd81aea3f59eac7128dba4b36d516c8"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Adding two inbound rules to the security group whose ID is **15457509-18f9-4387-bae6-d4ed1898b301** with duplicate rules ignored

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

import java.util.List;
import java.util.ArrayList;

public class BatchCreateSecurityGroupRulesSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
```

```
security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
environment variables and decrypted during use to ensure security.
// In this example, AK and SK are stored in environment variables for authentication. Before running
this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
String ak = System.getenv("CLOUD_SDK_AK");
String sk = System.getenv("CLOUD_SDK_SK");
String projectId = "{project_id}";

ICredential auth = new BasicCredentials()
    .withProjectId(projectId)
    .withAk(ak)
    .withSk(sk);

VpcClient client = VpcClient.newBuilder()
    .withCredential(auth)
    .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
    .build();
BatchCreateSecurityGroupRulesRequest request = new BatchCreateSecurityGroupRulesRequest();
request.withSecurityGroupId("{security_group_id}");
BatchCreateSecurityGroupRulesRequestBody body = new
BatchCreateSecurityGroupRulesRequestBody();
List<BatchCreateSecurityGroupRulesOption> listbodySecurityGroupRules = new ArrayList<>();
listbodySecurityGroupRules.add(
    new BatchCreateSecurityGroupRulesOption()
        .withDescription("")
        .withDirection("ingress")
        .withEthertype("IPv4")
        .withProtocol("tcp")
        .withMultiport("22")
        .withRemoteIpPrefix("117.78.12.122/32")
        .withAction("allow")
        .withPriority("1")
);
listbodySecurityGroupRules.add(
    new BatchCreateSecurityGroupRulesOption()
        .withDescription("")
        .withDirection("ingress")
        .withEthertype("IPv4")
        .withProtocol("tcp")
        .withMultiport("22")
        .withRemoteIpPrefix("117.78.12.122/32")
        .withAction("allow")
        .withPriority("1")
);
body.withIgnoreDuplicate(true);
body.withSecurityGroupRules(listbodySecurityGroupRules);
request.withBody(body);
try {
    BatchCreateSecurityGroupRulesResponse response = client.batchCreateSecurityGroupRules(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

Adding two inbound rules to the security group whose ID is **15457509-18f9-4387-bae6-d4ed1898b301** with duplicate rules ignored

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = BatchCreateSecurityGroupRulesRequest()
        request.security_group_id = "{security_group_id}"
        listSecurityGroupRulesbody = [
            BatchCreateSecurityGroupRulesOption(
                description="",
                direction="ingress",
                ethertype="IPv4",
                protocol="tcp",
                multiport="22",
                remote_ip_prefix="117.78.12.122/32",
                action="allow",
                priority="1"
            ),
            BatchCreateSecurityGroupRulesOption(
                description="",
                direction="ingress",
                ethertype="IPv4",
                protocol="tcp",
                multiport="22",
                remote_ip_prefix="117.78.12.122/32",
                action="allow",
                priority="1"
            )
        ]
        request.body = BatchCreateSecurityGroupRulesRequestBody(
            ignore_duplicate=True,
            security_group_rules=listSecurityGroupRulesbody
        )
        response = client.batch_create_security_group_rules(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Adding two inbound rules to the security group whose ID is **15457509-18f9-4387-bae6-d4ed1898b301** with duplicate rules ignored

```
package main
```

```
import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.BatchCreateSecurityGroupRulesRequest{}
    request.SecurityGroupId = "{security_group_id}"
    descriptionSecurityGroupRules:= ""
    ethertypeSecurityGroupRules:= "IPv4"
    protocolSecurityGroupRules:= "tcp"
    multiportSecurityGroupRules:= "22"
    remotelpPrefixSecurityGroupRules:= "117.78.12.122/32"
    actionSecurityGroupRules:= "allow"
    prioritySecurityGroupRules:= "1"
    descriptionSecurityGroupRules1:= ""
    ethertypeSecurityGroupRules1:= "IPv4"
    protocolSecurityGroupRules1:= "tcp"
    multiportSecurityGroupRules1:= "22"
    remotelpPrefixSecurityGroupRules1:= "117.78.12.122/32"
    actionSecurityGroupRules1:= "allow"
    prioritySecurityGroupRules1:= "1"
    var listSecurityGroupRulesbody = []model.BatchCreateSecurityGroupRulesOption{
        {
            Description: &descriptionSecurityGroupRules,
            Direction: "ingress",
            Ethertype: &ethertypeSecurityGroupRules,
            Protocol: &protocolSecurityGroupRules,
            Multiport: &multiportSecurityGroupRules,
            RemotelpPrefix: &remotelpPrefixSecurityGroupRules,
            Action: &actionSecurityGroupRules,
            Priority: &prioritySecurityGroupRules,
        },
        {
            Description: &descriptionSecurityGroupRules1,
            Direction: "ingress",
            Ethertype: &ethertypeSecurityGroupRules1,
            Protocol: &protocolSecurityGroupRules1,
            Multiport: &multiportSecurityGroupRules1,
            RemotelpPrefix: &remotelpPrefixSecurityGroupRules1,
            Action: &actionSecurityGroupRules1,
            Priority: &prioritySecurityGroupRules1,
        },
    }
    ignoreDuplicateBatchCreateSecurityGroupRulesRequestBody:= true
```

```
request.Body = &model.BatchCreateSecurityGroupRulesRequestBody{
    IgnoreDuplicate: &ignoreDuplicateBatchCreateSecurityGroupRulesRequestBody,
    SecurityGroupRules: listSecurityGroupRulesbody,
}
response, err := client.BatchCreateSecurityGroupRules(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
201	Normal response to the POST operation. For more status codes, see Status Codes .
202	Normal response for the specified pre-check request of API V3. For more status codes, see Status Code .

Error Codes

See [Error Codes](#).

5.4 IP Address Group

5.4.1 Creating an IP Address Group

Function

An IP address group is a collection of IP addresses. It can be associated with security groups and network ACLs to simplify IP address configuration and management in networking. You can create an IP address group to centrally manage IP address ranges and IP addresses.

Constraints

The default IP address group quota for each account is 50.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v3/{project_id}/vpc/address-groups

Table 5-79 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: ID of the project that an IP address group belongs to. For details about how to obtain a project ID, see Obtaining a Project ID . Range: N/A

Request Parameters

Table 5-80 Request body parameters

Parameter	Mandatory	Type	Description
dry_run	No	Boolean	Definition: Whether to only check the request. Constraints: N/A Range: • true: A check request will be sent and no IP address group will be created. Check items include mandatory parameters, request format, and constraints. If the check fails, an error will be returned. If the check succeeds, response code 202 will be returned. • false: A request will be sent and an IP address group will be created. Default Value: false

Parameter	Mandatory	Type	Description
address_group	Yes	CreateAddressGroupOption object	Definition: Request body for creating an IP address group. Constraints: N/A Range: N/A Default Value: N/A

Table 5-81 CreateAddressGroupOption

Parameter	Mandatory	Type	Description
name	Yes	String	Definition: The name of an IP address group. Constraints: The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods. Range: N/A Default Value: N/A
description	No	String	Definition: Description about an IP address group. Constraints: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >). Range: N/A Default Value: N/A

Parameter	Mandatory	Type	Description
ip_version	Yes	Integer	Definition: IP address version of an IP address group. Constraints: N/A Range: • 4: IPv4 address group • 6: IPv6 address group Default Value: N/A
max_capacity	No	Integer	Definition: Maximum number of IP address entries in an IP address group. Constraints: N/A Range: 0 to 20 Default Value: 20

Parameter	Mandatory	Type	Description
ip_set	No	Array of strings	Definition: IP address entries in an IP address group. Both IPv4 and IPv6 address entries are supported. Constraints: • The default maximum number of IP address sets, including IP addresses, IP address ranges, and CIDR blocks, in an IP address group is 20. • The ip_set and ip_extra_set parameters cannot be both specified in a request. If you need to add remarks for IP address entries, use the ip_extra_set parameter. Range: An IP address entry in an IP address set can be: • A single IP address, for example, 192.168.21.25 • An IP address range, for example, 192.168.21.25-192.168.21.30 • A CIDR block, for example, 192.168.21.0/24 Default Value: N/A

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Definition: ID of the enterprise project that an IP address group belongs to. This is the ID of enterprise project associated with the IP address group when you create the group. Constraints: • The value can contain a maximum of 36 bytes. • The value is 0 or a string in UUID format with hyphens (-). Range: N/A Default Value: 0 indicates the default enterprise project.
ip_extra_set	No	Array of IpExtraSetOption objects	Definition: IP address entries in an IP address group and their remarks. There are multiple IP address entry objects in an IP address group. Each IP address entry object contains one IP address entry and its remarks. An IP address entry is the same as that in ip_set . The remarks can describe the usage of the IP address entry. Constraints: • By default, the maximum number of IP address entry objects is 20. • The ip_set and ip_extra_set parameters cannot be both specified in a request. If you need to add remarks for IP address entries, use the ip_extra_set parameter. Range: N/A Default Value: N/A

Table 5-82 IpExtraSetOption

Parameter	Mandatory	Type	Description
ip	Yes	String	Definition: IP address entries in an IP address group. Both IPv4 and IPv6 address entries are supported. Constraints: N/A Range: • A single IP address, for example, 192.168.21.25 • An IP address range, for example, 192.168.21.25-192.168.21.30 • A CIDR block, for example, 192.168.21.0/24 Default Value: N/A
remarks	No	String	Definition: Remarks of an IP address entry. Constraints: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >). Range: N/A Default Value: N/A

Response Parameters

Status code: 201

Table 5-83 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Request ID. Range: N/A
address_group	AddressGroup object	Definition: Response body for creating an IP address group. Range: N/A

Table 5-84 AddressGroup

Parameter	Type	Description
id	String	Definition: ID of an IP address group. After an IP address group is created, an IP address group ID is generated, which uniquely identifies the IP address group. Range: The value is in UUID format with hyphens (-).
name	String	Definition: The name of an IP address group. Range: The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods.
description	String	Definition: Description about an IP address group. Range: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >).

Parameter	Type	Description
max_capacity	Integer	Definition: Maximum number of IP address entries in an IP address group. Range: The value can be from 0 to 20. The default value is 20.
ip_set	Array of strings	Definition: IP address entries in an IP address group. Both IPv4 and IPv6 address entries are supported. Range: An IP address entry in an IP address set can be: • A single IP address, for example, 192.168.21.25 • An IP address range, for example, 192.168.21.25-192.168.21.30 • A CIDR block, for example, 192.168.21.0/24
ip_version	Integer	Definition: IP address version of an IP address group. Range: • 4: IPv4 address group • 6: IPv6 address group
created_at	String	Definition: Time when an IP address group was created. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ss</i> .
updated_at	String	Definition: Time when an IP address group was last updated. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ss</i> .

Parameter	Type	Description
tenant_id	String	Definition: ID of the project that an IP address group belongs to. Range: N/A
enterprise_project_id	String	Definition: ID of the enterprise project that an IP address group belongs to. Range: The value is 0 or a string that contains a maximum of 36 characters in UUID format with hyphens (-). 0 indicates the default enterprise project.
tags	Array of ResponseTag objects	Definition: Tags of an IP address group, including tag keys and tag values, which can be used to classify and identify resources. For details, see the tag objects. Range: N/A
status	String	Definition: Status of an IP address group. If the IP address group is in the UPDATING state, it cannot be updated again. Range: • NORMAL: normal (default value) • UPDATING: being updated • UPDATE_FAILED: update failed
status_message	String	Definition: Details about the IP address group status. Range: N/A
ip_extra_set	Array of IpExtraSetResponseOption objects	Definition: IP address entries in an IP address group and their remarks. Range: N/A

Table 5-85 ResponseTag

Parameter	Type	Description
key	String	Definition: Tag key. Range: • A tag key can contain a maximum of 128 Unicode characters and cannot be left blank. • Each tag key of a resource must be unique. • The value can contain: – Letters – Digits – Special characters: underscores (_), hyphens (-) – Chinese characters
value	String	Definition: Tag value. Range: • Each value can contain a maximum of 255 Unicode characters and can be left blank. • The value can contain: – Letters – Digits – Special characters: underscores (_), hyphens (-), periods (.) – Chinese characters

Table 5-86 IpExtraSetRespOption

Parameter	Type	Description
ip	String	Definition: IP address entries in an IP address group. Both IPv4 and IPv6 address entries are supported. Range: - A single IP address, for example, 192.168.21.25 - An IP address range, for example, 192.168.21.25-192.168.21.30 - A CIDR block, for example, 192.168.21.0/24
remarks	String	Definition: Remarks of an IP address entry. Range: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >).

Example Requests

Create an IP address group named **AutoTester746010.580123789**, set the IP address 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",
    "enterprise_project_id": "0aad99bc-f5f6-4f78-8404-c598d76b0ed2",
    "max_capacity": 20
  }
}
```

Example Responses

Status code: 201

Normal response to the POST operation. For more status codes, see [Status Codes](#).

```
{
  "address_group": {
    "id": "dd18a501-fcd5-4adc-acfe-b0e2384baf08",
    "name": "AutoTester746010.580123789",
    "tenant_id": "b2782e6708b8475c993e6064bc456bf8",
    "ip_version": 4,
    "max_capacity": 20,
  }
}
```

```
"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
} ],
"enterprise_project_id" : "0aad99bc-f5f6-4f78-8404-c598d76b0ed2",
"created_at" : "2019-06-28T02:06:38.000+00:00",
"updated_at" : "2019-06-28T02:06:38.000+00:00",
"description" : "test",
"status" : "NORMAL",
"status_message" : "",
"tags" : [ ]
},
"request_id" : "f568db7a-2675-4271-8747-3e3f1c6381ba"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Create an IP address group named **AutoTester746010.580123789**, set the IP address 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.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

import java.util.List;
import java.util.ArrayList;

public class CreateAddressGroupSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
```

```
.withCredential(auth)
.withRegion(VpcRegion.valueOf("<YOUR REGION>"))
.build();
CreateAddressGroupRequest request = new CreateAddressGroupRequest();
CreateAddressGroupRequestBody body = new CreateAddressGroupRequestBody();
List<String> listAddressGroupIpSet = new ArrayList<>();
listAddressGroupIpSet.add("192.168.3.2");
listAddressGroupIpSet.add("192.168.3.40");
listAddressGroupIpSet.add("192.168.3.20-192.168.3.100");
listAddressGroupIpSet.add("192.168.5.0/24");
CreateAddressGroupOption addressGroupbody = new CreateAddressGroupOption();
addressGroupbody.withName("AutoTester746010.580123789")
.withDescription("test")
.withIpVersion(4)
.withIpSet(listAddressGroupIpSet)
.withMaxCapacity(20)
.withEnterpriseProjectId("0aad99bc-f5f6-4f78-8404-c598d76b0ed2");
body.withAddressGroup(addressGroupbody);
request.withBody(body);
try {
    CreateAddressGroupResponse response = client.createAddressGroup(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

Create an IP address group named **AutoTester746010.580123789**, set the IP address 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.

coding: utf-8

```
import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *
```

```
if __name__ == "__main__":
```

```
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
```

```
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
```

```
    ak = os.environ["CLOUD_SDK_AK"]
```

```
    sk = os.environ["CLOUD_SDK_SK"]
```

```
    projectId = "{project_id}"
```

```
    credentials = BasicCredentials(ak, sk, projectId)
```

```
    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.valueOf("<YOUR REGION>")) \
        .build()
```

```
    try:
```

```
request = CreateAddressGroupRequest()
listIpSetAddressGroup = [
    "192.168.3.2",
    "192.168.3.40",
    "192.168.3.20-192.168.3.100",
    "192.168.5.0/24"
]
addressGroupbody = CreateAddressGroupOption(
    name="AutoTester746010.580123789",
    description="test",
    ip_version=4,
    ip_set=listIpSetAddressGroup,
    max_capacity=20,
    enterprise_project_id="0aad99bc-f5f6-4f78-8404-c598d76b0ed2"
)
request.body = CreateAddressGroupRequestBody(
    address_group=addressGroupbody
)
response = client.create_address_group(request)
print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

Create an IP address group named **AutoTester746010.580123789**, set the IP address 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.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateAddressGroupRequest{}
    var listIpSetAddressGroup = []string{
        "192.168.3.2",
        "192.168.3.40",
        "192.168.3.20-192.168.3.100",
        "192.168.5.0/24"
    }
```

```
"192.168.3.20-192.168.3.100",
"192.168.5.0/24",
}
descriptionAddressGroup:= "test"
maxCapacityAddressGroup:= int32(20)
enterpriseProjectIdAddressGroup:= "0aad99bc-f5f6-4f78-8404-c598d76b0ed2"
addressGroupbody := &model.CreateAddressGroupOption{
    Name: "AutoTester746010.580123789",
    Description: &descriptionAddressGroup,
    IpVersion: int32(4),
    IpSet: &listIpSetAddressGroup,
    MaxCapacity: &maxCapacityAddressGroup,
    EnterpriseProjectId: &enterpriseProjectIdAddressGroup,
}
request.Body = &model.CreateAddressGroupRequestBody{
    AddressGroup: addressGroupbody,
}
response, err := client.CreateAddressGroup(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
201	Normal response to the POST operation. For more status codes, see Status Codes .

Error Codes

See [Error Codes](#).

5.4.2 Querying IP Address Groups

Function

This API is used to query information about all IP address groups, including the IP address group name and IP addresses.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v3/{project_id}/vpc/address-groups

Table 5-87 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: ID of the project that an IP address group belongs to. For details about how to obtain a project ID, see Obtaining a Project ID . Range: N/A

Table 5-88 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Definition: Number of resources on each page. Range: 0 to 2000
marker	No	String	Definition: Start resource ID of pagination query. If the parameter is left blank, only resources on the first page are queried. Range: ID of an IP address group.
id	No	Array of strings	Definition: ID of an IP address group. This field can be used to precisely filter IP address groups. Multiple IDs can be specified for filtering. Range: N/A
name	No	Array of strings	Definition: The name of an IP address group. This field can be used to precisely filter IP address groups. Multiple names can be specified for filtering. Range: N/A

Parameter	Mandatory	Type	Description
ip_version	No	Integer	Definition: IP address version of an IP address group. This field can be used to filter IP address groups. Range: • 4: IPv4 address groups will be filtered. • 6: IPv6 address groups will be filtered.
description	No	Array of strings	Definition: Description about an IP address group. This field can be used to precisely filter IP address groups. Multiple descriptions can be specified for filtering. Range: N/A
enterprise_project_id	No	String	Definition: ID of the enterprise project that an IP address group belongs to. This field can be used to filter the IP address groups of an enterprise project. Range: • The value is 0 or a string that contains a maximum of 36 characters in UUID format with hyphens (-). 0 indicates the default enterprise project. • To obtain the IP address groups associated with all enterprise projects that a user has permissions to view, specify all_granted_eps.

Request Parameters

None

Response Parameters

Status code: 200

Table 5-89 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Request ID. Range: N/A
address_groups	Array of AddressGroup objects	Definition: Response body for querying IP address groups. Range: N/A
page_info	PageInfo object	Definition: Pagination information. Range: N/A

Table 5-90 AddressGroup

Parameter	Type	Description
id	String	Definition: ID of an IP address group. After an IP address group is created, an IP address group ID is generated, which uniquely identifies the IP address group. Range: The value is in UUID format with hyphens (-).
name	String	Definition: The name of an IP address group. Range: The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods.

Parameter	Type	Description
description	String	Definition: Description about an IP address group. Range: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >).
max_capacity	Integer	Definition: Maximum number of IP address entries in an IP address group. Range: The value can be from 0 to 20. The default value is 20.
ip_set	Array of strings	Definition: IP address entries in an IP address group. Both IPv4 and IPv6 address entries are supported. Range: An IP address entry in an IP address set can be: • A single IP address, for example, 192.168.21.25 • An IP address range, for example, 192.168.21.25-192.168.21.30 • A CIDR block, for example, 192.168.21.0/24
ip_version	Integer	Definition: IP address version of an IP address group. Range: • 4: IPv4 address group • 6: IPv6 address group
created_at	String	Definition: Time when an IP address group was created. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ss</i> .

Parameter	Type	Description
updated_at	String	Definition: Time when an IP address group was last updated. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ss</i> .
tenant_id	String	Definition: ID of the project that an IP address group belongs to. Range: N/A
enterprise_project_id	String	Definition: ID of the enterprise project that an IP address group belongs to. Range: The value is 0 or a string that contains a maximum of 36 characters in UUID format with hyphens (-). 0 indicates the default enterprise project.
tags	Array of ResponseTag objects	Definition: Tags of an IP address group, including tag keys and tag values, which can be used to classify and identify resources. For details, see the tag objects. Range: N/A
status	String	Definition: Status of an IP address group. If the IP address group is in the UPDATING state, it cannot be updated again. Range: • NORMAL: normal (default value) • UPDATING: being updated • UPDATE_FAILED: update failed
status_message	String	Definition: Details about the IP address group status. Range: N/A

Parameter	Type	Description
ip_extra_set	Array of IpExtraSetRespOption objects	Definition: IP address entries in an IP address group and their remarks. Range: N/A

Table 5-91 ResponseTag

Parameter	Type	Description
key	String	Definition: Tag key. Range: - A tag key can contain a maximum of 128 Unicode characters and cannot be left blank. - Each tag key of a resource must be unique. - The value can contain: - Letters - Digits - Special characters: underscores (_), hyphens (-) - Chinese characters
value	String	Definition: Tag value. Range: - Each value can contain a maximum of 255 Unicode characters and can be left blank. - The value can contain: - Letters - Digits - Special characters: underscores (_), hyphens (-), periods (.) - Chinese characters

Table 5-92 IpExtraSetRespOption

Parameter	Type	Description
ip	String	Definition: IP address entries in an IP address group. Both IPv4 and IPv6 address entries are supported. Range: • A single IP address, for example, 192.168.21.25 • An IP address range, for example, 192.168.21.25-192.168.21.30 • A CIDR block, for example, 192.168.21.0/24
remarks	String	Definition: Remarks of an IP address entry. Range: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >).

Table 5-93 PageInfo

Parameter	Type	Description
previous_marker	String	Definition: The first record on the current page. Range: N/A
current_count	Integer	Definition: Total number of resources on the current page. Range: N/A
next_marker	String	Definition: The last record on the current page. The next_marker field does not exist if the page is the last one. Range: N/A

Example Requests

Query IP address groups based on combined filters.

```
GET https://{{endpoint}}/v3/b2782e6708b8475c993e6064bc456bf8/vpc/address-groups?name=ipGroup-test&description=test&ip_version=4
```

Example Responses

Status code: 200

Normal response to the GET operation. For more status codes, see [Status Codes](#).

```
{
  "address_groups": [ {
    "id": "dd18a501-fcd5-4adc-acfe-b0e2384baf08",
    "name": "ipGroup-test",
    "tenant_id": "b2782e6708b8475c993e6064bc456bf8",
    "ip_version": 4,
    "max_capacity": 20,
    "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
    } ],
    "enterprise_project_id": "0aad99bc-f5f6-4f78-8404-c598d76b0ed2",
    "created_at": "2019-06-28T02:06:38.000+00:00",
    "updated_at": "2019-06-28T02:06:38.000+00:00",
    "description": "test",
    "status": "NORMAL",
    "status_message": "",
    "tags": [ ]
  } ],
  "page_info": {
    "previous_marker": "dd18a501-fcd5-4adc-acfe-b0e2384baf08",
    "current_count": 1
  },
  "request_id": "e51fa17c-3259-4122-afb1-9c03d4ef5408"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;
```

```
public class ListAddressGroupSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();
        ListAddressGroupRequest request = new ListAddressGroupRequest();
        try {
            ListAddressGroupResponse response = client.listAddressGroup(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListAddressGroupRequest()
```



```
response = client.list_address_group(request)
print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListAddressGroupRequest{}
    response, err := client.ListAddressGroup(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Normal response to the GET operation. For more status codes, see Status Codes .

Error Codes

See [Error Codes](#).

5.4.3 Querying an IP Address Group

Function

This API is used to query information about an IP address group, including the IP address group name and IP addresses.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v3/{project_id}/vpc/address-groups/{address_group_id}

Table 5-94 Path Parameters

Parameter	Mandatory	Type	Description
address_group_id	Yes	String	Definition: ID of an IP address group. Range: N/A
project_id	Yes	String	Definition: ID of the project that an IP address group belongs to. For details about how to obtain a project ID, see Obtaining a Project ID . Range: N/A

Request Parameters

None

Response Parameters

Status code: 200

Table 5-95 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Request ID. Range: N/A
address_group	AddressGroup object	Definition: Response body for querying details about an IP address group. Range: N/A

Table 5-96 AddressGroup

Parameter	Type	Description
id	String	Definition: ID of an IP address group. After an IP address group is created, an IP address group ID is generated, which uniquely identifies the IP address group. Range: The value is in UUID format with hyphens (-).
name	String	Definition: The name of an IP address group. Range: The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods.
description	String	Definition: Description about an IP address group. Range: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >).

Parameter	Type	Description
max_capacity	Integer	Definition: Maximum number of IP address entries in an IP address group. Range: The value can be from 0 to 20. The default value is 20.
ip_set	Array of strings	Definition: IP address entries in an IP address group. Both IPv4 and IPv6 address entries are supported. Range: An IP address entry in an IP address set can be: • A single IP address, for example, 192.168.21.25 • An IP address range, for example, 192.168.21.25-192.168.21.30 • A CIDR block, for example, 192.168.21.0/24
ip_version	Integer	Definition: IP address version of an IP address group. Range: • 4: IPv4 address group • 6: IPv6 address group
created_at	String	Definition: Time when an IP address group was created. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ss</i> .
updated_at	String	Definition: Time when an IP address group was last updated. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ss</i> .

Parameter	Type	Description
tenant_id	String	Definition: ID of the project that an IP address group belongs to. Range: N/A
enterprise_project_id	String	Definition: ID of the enterprise project that an IP address group belongs to. Range: The value is 0 or a string that contains a maximum of 36 characters in UUID format with hyphens (-). 0 indicates the default enterprise project.
tags	Array of ResponseTag objects	Definition: Tags of an IP address group, including tag keys and tag values, which can be used to classify and identify resources. For details, see the tag objects. Range: N/A
status	String	Definition: Status of an IP address group. If the IP address group is in the UPDATING state, it cannot be updated again. Range: • NORMAL: normal (default value) • UPDATING: being updated • UPDATE_FAILED: update failed
status_message	String	Definition: Details about the IP address group status. Range: N/A
ip_extra_set	Array of IpExtraSetResponseOption objects	Definition: IP address entries in an IP address group and their remarks. Range: N/A

Table 5-97 ResponseTag

Parameter	Type	Description
key	String	Definition: Tag key. Range: • A tag key can contain a maximum of 128 Unicode characters and cannot be left blank. • Each tag key of a resource must be unique. • The value can contain: – Letters – Digits – Special characters: underscores (_), hyphens (-) – Chinese characters
value	String	Definition: Tag value. Range: • Each value can contain a maximum of 255 Unicode characters and can be left blank. • The value can contain: – Letters – Digits – Special characters: underscores (_), hyphens (-), periods (.) – Chinese characters

Table 5-98 IpExtraSetRespOption

Parameter	Type	Description
ip	String	Definition: IP address entries in an IP address group. Both IPv4 and IPv6 address entries are supported. Range: • A single IP address, for example, 192.168.21.25 • An IP address range, for example, 192.168.21.25-192.168.21.30 • A CIDR block, for example, 192.168.21.0/24
remarks	String	Definition: Remarks of an IP address entry. Range: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >).

Example Requests

Querying the details of an IP address group

```
GET https://{Endpoint}/v3/2bc7a67b35a64a79ad1d3bb8b5f61fc9/vpc/address-groups/dd18a501-fcd5-4adc-acfe-b0e2384baf08
```

Example Responses

Status code: 200

Normal response to the GET operation. For more status codes, see [Status Codes](#).

```
{
  "address_group": {
    "id": "dd18a501-fcd5-4adc-acfe-b0e2384baf08",
    "name": "AutoTester746010.580123789",
    "tenant_id": "b2782e6708b8475c993e6064bc456bf8",
    "ip_version": 4,
    "max_capacity": 20,
    "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
    }
  ]
}
```

```
    } ],  
    "enterprise_project_id" : "0aad99bc-f5f6-4f78-8404-c598d76b0ed2",  
    "created_at" : "2019-06-28T02:06:38.000+00:00",  
    "updated_at" : "2019-06-28T02:06:38.000+00:00",  
    "description" : "10.10.4.0/23",  
    "status" : "NORMAL",  
    "status_message" : "",  
    "tags" : [ ]  
  },  
  "request_id" : "ce6c359b-9002-41e5-a0b1-232759bd6637"  
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;  
  
import com.huaweicloud.sdk.core.auth.ICredential;  
import com.huaweicloud.sdk.core.auth.BasicCredentials;  
import com.huaweicloud.sdk.core.exception.ConnectionException;  
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;  
import com.huaweicloud.sdk.core.exception.ServiceResponseException;  
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;  
import com.huaweicloud.sdk.vpc.v3.*;  
import com.huaweicloud.sdk.vpc.v3.model.*;  
  
public class ShowAddressGroupSolution {  
  
    public static void main(String[] args) {  
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great  
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or  
        // environment variables and decrypted during use to ensure security.  
        // In this example, AK and SK are stored in environment variables for authentication. Before running  
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
        String ak = System.getenv("CLOUD_SDK_AK");  
        String sk = System.getenv("CLOUD_SDK_SK");  
        String projectId = "{project_id}";  
  
        ICredential auth = new BasicCredentials()  
            .withProjectId(projectId)  
            .withAk(ak)  
            .withSk(sk);  
  
        VpcClient client = VpcClient.newBuilder()  
            .withCredential(auth)  
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))  
            .build();  
        ShowAddressGroupRequest request = new ShowAddressGroupRequest();  
        request.withAddressGroupId("{address_group_id}");  
        try {  
            ShowAddressGroupResponse response = client.showAddressGroup(request);  
            System.out.println(response.toString());  
        } catch (ConnectionException e) {  
            e.printStackTrace();  
        } catch (RequestTimeoutException e) {  
            e.printStackTrace();  
        } catch (ServiceResponseException e) {  
            e.printStackTrace();  
            System.out.println(e.getStatusCode());  
            System.out.println(e.getRequestId());  
            System.out.println(e.getErrorCode());  
            System.out.println(e.getErrMsg());  
        }  
    }  
}
```



```
}  
}
```

Python

```
# coding: utf-8  
  
import os  
from huaweicloudsdkcore.auth.credentials import BasicCredentials  
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion  
from huaweicloudsdkcore.exceptions import exceptions  
from huaweicloudsdkvpc.v3 import *  
  
if __name__ == "__main__":  
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security  
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment  
    # variables and decrypted during use to ensure security.  
    # In this example, AK and SK are stored in environment variables for authentication. Before running this  
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak = os.environ["CLOUD_SDK_AK"]  
    sk = os.environ["CLOUD_SDK_SK"]  
    projectId = "{project_id}"  
  
    credentials = BasicCredentials(ak, sk, projectId)  
  
    client = VpcClient.new_builder() \  
        .with_credentials(credentials) \  
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \  
        .build()  
  
    try:  
        request = ShowAddressGroupRequest()  
        request.address_group_id = "{address_group_id}"  
        response = client.show_address_group(request)  
        print(response)  
    except exceptions.ClientRequestException as e:  
        print(e.status_code)  
        print(e.request_id)  
        print(e.error_code)  
        print(e.error_msg)
```

Go

```
package main  
  
import (  
    "fmt"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"  
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"  
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"  
)  
  
func main() {  
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security  
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment  
    // variables and decrypted during use to ensure security.  
    // In this example, AK and SK are stored in environment variables for authentication. Before running this  
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak := os.Getenv("CLOUD_SDK_AK")  
    sk := os.Getenv("CLOUD_SDK_SK")  
    projectId := "{project_id}"  
  
    auth := basic.NewCredentialsBuilder().  
        WithAk(ak).  
        WithSk(sk).  
        WithProjectId(projectId).  
        Build()
```

```
client := vpc.NewVpcClient(  
    vpc.VpcClientBuilder().  
        WithRegion(region.ValueOf("<YOUR REGION>")).  
        WithCredential(auth).  
        Build())  
  
request := &model.ShowAddressGroupRequest{  
    request.AddressGroupId = "{address_group_id}"  
}  
response, err := client.ShowAddressGroup(request)  
if err == nil {  
    fmt.Printf("%+v\n", response)  
} else {  
    fmt.Println(err)  
}  
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Normal response to the GET operation. For more status codes, see Status Codes .

Error Codes

See [Error Codes](#).

5.4.4 Updating an IP Address Group

Function

This API is used to update information about an IP address group, including the IP address group name and IP addresses.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v3/{project_id}/vpc/address-groups/{address_group_id}

Table 5-99 Path Parameters

Parameter	Mandatory	Type	Description
address_group_id	Yes	String	Definition: ID of an IP address group. Range: N/A
project_id	Yes	String	Definition: ID of the project that an IP address group belongs to. For details about how to obtain a project ID, see Obtaining a Project ID . Range: N/A

Request Parameters

Table 5-100 Request body parameters

Parameter	Mandatory	Type	Description
dry_run	No	Boolean	Definition: Whether to only check the request. Constraints: N/A Range: true: A check request will be sent and the IP address group will not be updated. Check items include mandatory parameters, request format, and constraints. If the check fails, an error will be returned. If the check succeeds, response code 202 will be returned. false: A request will be sent and the IP address group will be updated. Default Value: false

Parameter	Mandatory	Type	Description
address_group	Yes	UpdateAddressGroupOption object	Definition: Request body for updating an IP address group. Constraints: N/A Range: N/A Default Value: N/A

Table 5-101 UpdateAddressGroupOption

Parameter	Mandatory	Type	Description
name	No	String	Definition: The name of an IP address group. Constraints: The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods. Range: N/A Default Value: N/A
description	No	String	Definition: Description about an IP address group. Constraints: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >). Range: N/A Default Value: N/A

Parameter	Mandatory	Type	Description
ip_set	No	Array of strings	Definition: IP address entries in an IP address group. Both IPv4 and IPv6 address entries are supported. Constraints: • 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_set and ip_extra_set cannot be both specified in a request. Range: An IP address entry in an IP address set can be: • A single IP address, for example, 192.168.21.25 • An IP address range, for example, 192.168.21.25-192.168.21.30 • A CIDR block, for example, 192.168.21.0/24 Default Value: N/A
max_capacity	No	Integer	Definition: Maximum number of IP address entries in an IP address group. Constraints: N/A Range: 0 to 20 Default Value: 20

Parameter	Mandatory	Type	Description
ip_extra_set	No	Array of IpExtraSetOption objects	Definition: IP address entries in an IP address group and their remarks. Constraints: - By default, the maximum number of IP address entries is 20. ip_set and ip_extra_set cannot be both specified in a request. Range: N/A Default Value: N/A

Table 5-102 IpExtraSetOption

Parameter	Mandatory	Type	Description
ip	Yes	String	Definition: IP address entries in an IP address group. Both IPv4 and IPv6 address entries are supported. Constraints: N/A Range: - A single IP address, for example, 192.168.21.25 - An IP address range, for example, 192.168.21.25-192.168.21.30 - A CIDR block, for example, 192.168.21.0/24 Default Value: N/A

Parameter	Mandatory	Type	Description
remarks	No	String	Definition: Remarks of an IP address entry. Constraints: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >). Range: N/A Default Value: N/A

Response Parameters

Status code: 200

Table 5-103 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Request ID. Range: N/A
address_group	AddressGroup object	Definition: Response body for updating an IP address group. Range: N/A

Table 5-104 AddressGroup

Parameter	Type	Description
id	String	Definition: ID of an IP address group. After an IP address group is created, an IP address group ID is generated, which uniquely identifies the IP address group. Range: The value is in UUID format with hyphens (-).
name	String	Definition: The name of an IP address group. Range: The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods.
description	String	Definition: Description about an IP address group. Range: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >).
max_capacity	Integer	Definition: Maximum number of IP address entries in an IP address group. Range: The value can be from 0 to 20. The default value is 20.
ip_set	Array of strings	Definition: IP address entries in an IP address group. Both IPv4 and IPv6 address entries are supported. Range: An IP address entry in an IP address set can be: • A single IP address, for example, 192.168.21.25 • An IP address range, for example, 192.168.21.25-192.168.21.30 • A CIDR block, for example, 192.168.21.0/24

Parameter	Type	Description
ip_version	Integer	Definition: IP address version of an IP address group. Range: • 4: IPv4 address group • 6: IPv6 address group
created_at	String	Definition: Time when an IP address group was created. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ss</i> .
updated_at	String	Definition: Time when an IP address group was last updated. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ss</i> .
tenant_id	String	Definition: ID of the project that an IP address group belongs to. Range: N/A
enterprise_project_id	String	Definition: ID of the enterprise project that an IP address group belongs to. Range: The value is 0 or a string that contains a maximum of 36 characters in UUID format with hyphens (-). 0 indicates the default enterprise project.
tags	Array of ResponseTag objects	Definition: Tags of an IP address group, including tag keys and tag values, which can be used to classify and identify resources. For details, see the tag objects. Range: N/A

Parameter	Type	Description
status	String	Definition: Status of an IP address group. If the IP address group is in the UPDATING state, it cannot be updated again. Range: • NORMAL: normal (default value) • UPDATING: being updated • UPDATE_FAILED: update failed
status_message	String	Definition: Details about the IP address group status. Range: N/A
ip_extra_set	Array of IpExtraSetRespOption objects	Definition: IP address entries in an IP address group and their remarks. Range: N/A

Table 5-105 ResponseTag

Parameter	Type	Description
key	String	Definition: Tag key. Range: • A tag key can contain a maximum of 128 Unicode characters and cannot be left blank. • Each tag key of a resource must be unique. • The value can contain: – Letters – Digits – Special characters: underscores (_), hyphens (-) – Chinese characters

Parameter	Type	Description
value	String	Definition: Tag value. Range: - Each value can contain a maximum of 255 Unicode characters and can be left blank. - The value can contain: - Letters - Digits - Special characters: underscores (_), hyphens (-), periods (.) - Chinese characters

Table 5-106 IpExtraSetRespOption

Parameter	Type	Description
ip	String	Definition: IP address entries in an IP address group. Both IPv4 and IPv6 address entries are supported. Range: - A single IP address, for example, 192.168.21.25 - An IP address range, for example, 192.168.21.25-192.168.21.30 - A CIDR block, for example, 192.168.21.0/24
remarks	String	Definition: Remarks of an IP address entry. Range: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >).

Example Requests

Change the IP set and description of the IP address group whose ID is **dd18a501-fcd5-4adc-acfe-b0e2384baf08**. Change the IP address group name to **vkvgkykvsjhjaaaa1**.

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": "xxxxxxxxx"
  }
}
```

Example Responses

Status code: 200

Normal response to the PUT operation. For more status codes, see [Status Codes](#).

```
{
  "address_group": {
    "id": "dd18a501-fcd5-4adc-acfe-b0e2384baf08",
    "name": "vkvgykvsvhjaaaa1",
    "tenant_id": "b2782e6708b8475c993e6064bc456bf8",
    "ip_version": 4,
    "max_capacity": 20,
    "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
    } ],
    "enterprise_project_id": "0aad99bc-f5f6-4f78-8404-c598d76b0ed2",
    "created_at": "2019-06-28T02:06:38.000+00:00",
    "updated_at": "2019-06-28T02:14:01.000+00:00",
    "description": "xxxxxxxxx",
    "status": "NORMAL",
    "status_message": "",
    "tags": [ ]
  },
  "request_id": "5bbd1640-fa68-4362-9a5c-30c4809958e0"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Change the IP set and description of the IP address group whose ID is **dd18a501-fcd5-4adc-acfe-b0e2384baf08**. Change the IP address group name to **vkvgykvsvhjaaaa1**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
```

```
import com.huaweicloud.sdk.vpc.v3.model.*;

import java.util.List;
import java.util.ArrayList;

public class UpdateAddressGroupSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();

        UpdateAddressGroupRequest request = new UpdateAddressGroupRequest();
        request.withAddressGroupId("{address_group_id}");
        UpdateAddressGroupRequestBody body = new UpdateAddressGroupRequestBody();
        List<String> listAddressGroupIpSet = new ArrayList<>();
        listAddressGroupIpSet.add("192.168.3.2");
        listAddressGroupIpSet.add("192.168.3.43");
        listAddressGroupIpSet.add("192.168.3.20-192.168.3.100");
        listAddressGroupIpSet.add("192.168.5.0/24");
        UpdateAddressGroupOption addressGroupbody = new UpdateAddressGroupOption();
        addressGroupbody.withName("vkvgykvsvhjaaaa1")
            .withDescription("xxxxxxxxxx")
            .withIpSet(listAddressGroupIpSet);
        body.withAddressGroup(addressGroupbody);
        request.withBody(body);
        try {
            UpdateAddressGroupResponse response = client.updateAddressGroup(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrMsg());
        }
    }
}
```

Python

Change the IP set and description of the IP address group whose ID is **dd18a501-fcd5-4adc-acfe-b0e2384baf08**. Change the IP address group name to **vkvgykvsvhjaaaa1**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
```

```
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdateAddressGroupRequest()
        request.address_group_id = "{address_group_id}"
        listIpSetAddressGroup = [
            "192.168.3.2",
            "192.168.3.43",
            "192.168.3.20-192.168.3.100",
            "192.168.5.0/24"
        ]
        addressGroupbody = UpdateAddressGroupOption(
            name="vkvgykvsjhjaaaa1",
            description="xxxxxxxxxx",
            ip_set=listIpSetAddressGroup
        )
        request.body = UpdateAddressGroupRequestBody(
            address_group=addressGroupbody
        )
        response = client.update_address_group(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Change the IP set and description of the IP address group whose ID is **dd18a501-fcd5-4adc-acfe-b0e2384baf08**. Change the IP address group name to **vkvgykvsjhjaaaa1**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
```

```
sk := os.Getenv("CLOUD_SDK_SK")
projectId := "{project_id}"

auth := basic.NewCredentialsBuilder().
    WithAk(ak).
    WithSk(sk).
    WithProjectId(projectId).
    Build()

client := vpc.NewVpcClient(
    vpc.VpcClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.UpdateAddressGroupRequest{}
request.AddressGroupId = "{address_group_id}"
var listIpSetAddressGroup = []string{
    "192.168.3.2",
    "192.168.3.43",
    "192.168.3.20-192.168.3.100",
    "192.168.5.0/24",
}
nameAddressGroup:= "vkvgykvsvhjaaaa1"
descriptionAddressGroup:= "xxxxxxxxxx"
addressGroupbody := &model.UpdateAddressGroupOption{
    Name: &nameAddressGroup,
    Description: &descriptionAddressGroup,
    IpSet: &listIpSetAddressGroup,
}
request.Body = &model.UpdateAddressGroupRequestBody{
    AddressGroup: addressGroupbody,
}
response, err := client.UpdateAddressGroup(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Normal response to the PUT operation. For more status codes, see Status Codes .

Error Codes

See [Error Codes](#).

5.4.5 Deleting an IP Address Group

Function

This API can be used to delete an IP address group that is no longer used. This API does not forcibly delete an IP address group. Before deleting an IP address group, ensure that no resource is using this group.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v3/{project_id}/vpc/address-groups/{address_group_id}

Table 5-107 Path Parameters

Parameter	Mandatory	Type	Description
address_group_id	Yes	String	Definition: ID of an IP address group. Range: N/A
project_id	Yes	String	Definition: ID of the project that an IP address group belongs to. For details about how to obtain a project ID, see Obtaining a Project ID . Range: N/A

Request Parameters

None

Response Parameters

Status code: 204

Normal response to the DELETE operation. For more status codes, see [Status Codes](#).

None

Example Requests

Delete the IP address group whose ID is **dd18a501-fcd5-4adc-acfe-b0e2384baf08**.

```
DELETE https://{endpoint}/v3/{tenant_id}/vpc/address-groups/dd18a501-fcd5-4adc-acfe-b0e2384baf08
```

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class DeleteAddressGroupSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();
        DeleteAddressGroupRequest request = new DeleteAddressGroupRequest();
        request.withAddressGroupId("{address_group_id}");
        try {
            DeleteAddressGroupResponse response = client.deleteAddressGroup(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

```
}  
}
```

Python

```
# coding: utf-8  
  
import os  
from huaweicloudsdkcore.auth.credentials import BasicCredentials  
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion  
from huaweicloudsdkcore.exceptions import exceptions  
from huaweicloudsdkvpc.v3 import *  
  
if __name__ == "__main__":  
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security  
    risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment  
    variables and decrypted during use to ensure security.  
    # In this example, AK and SK are stored in environment variables for authentication. Before running this  
    example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak = os.environ["CLOUD_SDK_AK"]  
    sk = os.environ["CLOUD_SDK_SK"]  
    projectId = "{project_id}"  
  
    credentials = BasicCredentials(ak, sk, projectId)  
  
    client = VpcClient.new_builder() \  
        .with_credentials(credentials) \  
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \  
        .build()  
  
    try:  
        request = DeleteAddressGroupRequest()  
        request.address_group_id = "{address_group_id}"  
        response = client.delete_address_group(request)  
        print(response)  
    except exceptions.ClientRequestException as e:  
        print(e.status_code)  
        print(e.request_id)  
        print(e.error_code)  
        print(e.error_msg)
```

Go

```
package main  
  
import (  
    "fmt"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"  
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"  
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"  
)  
  
func main() {  
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security  
    risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment  
    variables and decrypted during use to ensure security.  
    // In this example, AK and SK are stored in environment variables for authentication. Before running this  
    example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak := os.Getenv("CLOUD_SDK_AK")  
    sk := os.Getenv("CLOUD_SDK_SK")  
    projectId := "{project_id}"  
  
    auth := basic.NewCredentialsBuilder().  
        WithAk(ak).  
        WithSk(sk).  
        WithProjectId(projectId).  
        Build()
```

```
client := vpc.NewVpcClient(  
    vpc.VpcClientBuilder().  
        WithRegion(region.ValueOf("<YOUR REGION>")).  
        WithCredential(auth).  
        Build())  
  
request := &model.DeleteAddressGroupRequest{  
    request.AddressGroupId = "{address_group_id}"  
    response, err := client.DeleteAddressGroup(request)  
    if err == nil {  
        fmt.Printf("%+v\n", response)  
    } else {  
        fmt.Println(err)  
    }  
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
204	Normal response to the DELETE operation. For more status codes, see Status Codes .

Error Codes

See [Error Codes](#).

5.4.6 Forcibly Deleting an IP Address Group

Function

You can call this API to delete an IP address group that is no longer used. This API is used to forcibly delete an IP address group. If the IP address group to be deleted is associated with security group rules or network ACL rules, the IP address group and its associated rules will be deleted together.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v3/{project_id}/vpc/address-groups/{address_group_id}/force

Table 5-108 Path Parameters

Parameter	Mandatory	Type	Description
address_group_id	Yes	String	Definition: ID of an IP address group. Range: N/A
project_id	Yes	String	Definition: ID of the project that an IP address group belongs to. For details about how to obtain a project ID, see Obtaining a Project ID . Range: N/A

Request Parameters

None

Response Parameters

Status code: 204

Normal response to the DELETE operation. For more status codes, see [Status Codes](#).

None

Example Requests

Forcibly delete the address group whose ID is **dd18a501-fcd5-4adc-acfe-b0e2384baf08**.

```
DELETE https://{endpoint}/v3/{tenant_id}/vpc/address-groups/dd18a501-fcd5-4adc-acfe-b0e2384baf08/force
```

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
```

```
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class DeleteIpAddressGroupForceSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();
        DeleteIpAddressGroupForceRequest request = new DeleteIpAddressGroupForceRequest();
        request.withAddressGroupId("{address_group_id}");
        try {
            DeleteIpAddressGroupForceResponse response = client.deleteIpAddressGroupForce(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)
```

```
client = VpcClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(VpcRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = DeletelpAddressGroupForceRequest()
    request.address_group_id = "{address_group_id}"
    response = client.delete_ip_address_group_force(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeletelpAddressGroupForceRequest{}
    request.AddressGroupId = "{address_group_id}"
    response, err := client.DeleteIpAddressGroupForce(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
204	Normal response to the DELETE operation. For more status codes, see Status Codes .

Error Codes

See [Error Codes](#).

5.5 Supplementary Network Interface

5.5.1 Creating a Supplementary Network Interface

Function

Supplementary network interfaces can be attached to an elastic network interface to allow a cloud server to have more network interfaces for flexible and high-availability network configuration.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v3/{project_id}/vpc/sub-network-interfaces

Table 5-109 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: ID of the project that a supplementary network interface belongs to. For details about how to obtain a project ID, see Obtaining a Project ID . Range: N/A

Request Parameters

Table 5-110 Request body parameters

Parameter	Mandatory	Type	Description
dry_run	No	Boolean	Definition: Whether to only check the request. Constraints: N/A Range: true: A check request will be sent and no supplementary network interface will be created. Check items include mandatory parameters, request format, and constraints. If the check fails, an error will be returned. If the check succeeds, response code 202 will be returned. false: A request will be sent and a supplementary network interface will be created. Default Value: false
sub_network_interface	Yes	CreateSubNetworkInterfaceOption object	Definition: Request body for creating a supplementary network interface. Constraints: N/A Range: N/A Default Value: N/A

Table 5-111 CreateSubNetworkInterfaceOption

Parameter	Mandatory	Type	Description
virsubnet_id	Yes	String	Definition: ID of the virtual subnet that a supplementary network interface is located. Constraints: The value is in UUID format with hyphens (-). Range: N/A Default Value: N/A
vlan_id	No	String	Definition: VLAN ID of a supplementary network interface. Constraints: The VLAN IDs of supplementary network interfaces attached to the same network interface must be unique. Range: 1 to 4094 Default Value: N/A
parent_id	Yes	String	Definition: ID of the elastic network interface that a supplementary network interface is attached to. Constraints: The value must be an existing elastic network interface ID. Range: N/A Default Value: N/A

Parameter	Mandatory	Type	Description
description	No	String	Definition: Description of a supplementary network interface. Constraints: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >). Range: N/A Default Value: N/A
ipv6_enable	No	Boolean	Definition: Whether IPv6 is enabled for a supplementary network interface. Constraints: N/A Range: • true: IPv6 is enabled. • false: IPv6 is disabled. Default Value: false
private_ip_address	No	String	Definition: Private IPv4 address of a supplementary network interface. Constraints: The value must be in the virtual subnet. If this parameter is left blank, an IP address will be randomly assigned from the virtual subnet. Range: N/A Default Value: N/A

Parameter	Mandatory	Type	Description
ipv6_ip_addresses	No	String	Definition: Private IPv6 address of a supplementary network interface. Constraints: The value must be in the virtual subnet. If this parameter is left blank, an IP address will be randomly assigned from the virtual subnet. Range: N/A Default Value: N/A
security_groups	No	Array of strings	Definition: IDs of the security groups that a supplementary network interface is associated with. For example, "security_groups": ["a0608cbf-d047-4f54-8b28-cd7b59853fff"]. Constraints: If this parameter is not specified in the request, the supplementary network interface is automatically associated with the default security group after being created. Range: N/A Default Value: N/A

Parameter	Mandatory	Type	Description
project_id	No	String	Definition: ID of the project that a supplementary network interface belongs to. Constraints: This parameter can only be set to the tenant ID of the current tenant. If this parameter is not specified, the project ID of the current tenant is used by default. Range: N/A Default Value: N/A
allowed_address_pairs	No	Array of AllowedAddressPair objects	Definition: IP/MAC address pair list of a supplementary network interface. For details, see the AllowedAddressPair object list. Constraints: • Configure a dedicated security group if a large CIDR block (subnet mask less than 24) is configured for parameter allowed_address_pairs. • In the hardware SDN networking plan, the ip_address attribute value cannot be in CIDR format. Range: N/A Default Value: N/A

Table 5-112 AllowedAddressPair

Parameter	Mandatory	Type	Description
ip_address	No	String	Definition: IP address. Constraints: Configure a dedicated security group if a large CIDR block (subnet mask less than 24) is configured for parameter allowed_address_pairs . Range: Single IP address, for example, 192.168.21.25 A CIDR block, for example, 192.168.21.0/24 Default Value: N/A
mac_address	No	String	Definition: MAC address. Constraints: N/A Range: N/A Default Value: N/A

Response Parameters

Status code: 201

Table 5-113 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Request ID. Range: N/A

Parameter	Type	Description
sub_network_interface	SubNetworkInterface object	Definition: Response body for creating a supplementary network interface. Range: N/A

Table 5-114 SubNetworkInterface

Parameter	Type	Description
id	String	Definition: ID of a supplementary network interface. After a supplementary network interface is created, a supplementary network interface ID is generated, which uniquely identifies the supplementary network interface. Range: The value is in UUID format with hyphens (-).
virsubnet_id	String	Definition: ID of the virtual subnet that a supplementary network interface is located. Range: The value is in UUID format with hyphens (-).
private_ip_address	String	Definition: Private IPv4 address of a supplementary network interface. Range: N/A
ipv6_ip_address	String	Definition: Private IPv6 address of a supplementary network interface. Range: N/A

Parameter	Type	Description
mac_address	String	Definition: MAC address of a supplementary network interface. Range: The value is a valid MAC address assigned by the system randomly.
parent_device_id	String	Definition: Device ID of the host network interface that a supplementary network interface is attached to. Range: The value is in UUID format with hyphens (-).
parent_id	String	Definition: ID of the elastic network interface that a supplementary network interface is attached to. Range: The value is in UUID format with hyphens (-).
description	String	Definition: Description of a supplementary network interface. Range: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >).
vpc_id	String	Definition: ID of the VPC that a supplementary network interface belongs to. Range: The value is in UUID format with hyphens (-).
vlan_id	Integer	Definition: VLAN ID of a supplementary network interface. Range: 1 to 4094

Parameter	Type	Description
security_groups	Array of strings	Definition: IDs of the security groups that a supplementary network interface is associated with. For example, "security_groups": ["a0608cbf-d047-4f54-8b28-cd7b59853fff"]. Range: If this parameter is not specified in the request, the supplementary network interface is automatically associated with the default security group after being created.
tags	Array of ResponseTag objects	Definition: Tags of a supplementary network interface, including tag keys and tag values, which can be used to classify and identify resources. For details, see the tag objects. Range: N/A
project_id	String	Definition: ID of the project that a supplementary network interface belongs to. Range: N/A
created_at	String	Definition: Time when a supplementary network interface was created. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .
allowed_address_pairs	Array of AllowedAddressPair objects	Definition: IP/MAC address pair list of a supplementary network interface. For details, see the AllowedAddressPair object list. Range: N/A

Parameter	Type	Description
state	String	Definition: Status of a supplementary network interface. Range: • NORMAL: The supplementary network interface is attached to an elastic network interface. • UNBOUND: The supplementary network interface is not attached to an elastic network interface.
instance_id	String	Definition: ID of the cloud service instance that a supplementary network interface is attached to, for example, RDS instance ID. Range: N/A
instance_type	String	Definition: Type of the cloud service instance that a supplementary network interface is attached to, for example, RDS. Range: N/A
scope	String	Definition: Public network egress information of the site where a supplementary network interface works. Range: • center: default value, indicating the central AZ. • AZ ID: a specific AZ
security_enabled	Boolean	Definition: Whether the security option is enabled for a supplementary network interface. If the option is not enabled, the security group does not take effect. Range: N/A

Table 5-115 ResponseTag

Parameter	Type	Description
key	String	Definition: Tag key. Range: • A tag key can contain a maximum of 128 Unicode characters and cannot be left blank. • Each tag key of a resource must be unique. • The value can contain: – Letters – Digits – Special characters: underscores (_), hyphens (-) – Chinese characters
value	String	Definition: Tag value. Range: • Each value can contain a maximum of 255 Unicode characters and can be left blank. • The value can contain: – Letters – Digits – Special characters: underscores (_), hyphens (-), periods (.) – Chinese characters

Table 5-116 AllowedAddressPair

Parameter	Type	Description
ip_address	String	Definition: IP address. Constraints: Configure a dedicated security group if a large CIDR block (subnet mask less than 24) is configured for parameter allowed_address_pairs . Range: Single IP address, for example, 192.168.21.25 A CIDR block, for example, 192.168.21.0/24 Default Value: N/A
mac_address	String	Definition: MAC address. Constraints: N/A Range: N/A Default Value: N/A

Example Requests

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 Responses

Status code: 201

Normal response to the POST operation. For more status codes, see [Status Codes](#).

```
{
  "sub_network_interface" : {
    "id" : "1f5fca65-6a75-47c8-942b-db1bbb81a22a",
    "project_id" : "8c6fb137a48a428aaf9a0229dca4edb3",
    "virsubnet_id" : "08278e6c-61ca-46c1-9fc3-0d4f6c12f193",
    "private_ip_address" : "192.168.0.219",
    "ipv6_ip_address" : "2407:c080:1200:2038:53a4:ad1c:ef34:f4ef",
    "mac_address" : "fa:16:3e:26:7e:59",
    "parent_device_id" : "285b2e45-2968-4f4c-8992-54e0d4c8da1d",
    "security_enabled" : true,
    "security_groups" : [ "6727c950-9f01-47a2-a7aa-7d3686c4c95b" ],
    "allowed_address_pairs" : [ ],
    "vpc_id" : "c10e1e02-9db2-4bd0-89ef-52536952627e",
    "instance_id" : "",
    "instance_type" : "",
    "description" : "",
    "parent_id" : "637748df-2986-4350-8303-95d259580fb3",
    "vlan_id" : 551,
    "state" : "NORMAL",
    "tags" : [ ],
    "scope" : "center",
    "created_at" : "2025-02-10T08:17:16Z"
  },
  "request_id" : "f0893730b622bf32beea6fa5b387a5dc"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

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.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

import java.util.List;
import java.util.ArrayList;

public class CreateSubNetworkInterfaceSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);
```

```
VpcClient client = VpcClient.newBuilder()
    .withCredential(auth)
    .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
    .build();
CreateSubNetworkInterfaceRequest request = new CreateSubNetworkInterfaceRequest();
CreateSubNetworkInterfaceRequestBody body = new CreateSubNetworkInterfaceRequestBody();
List<String> listSubNetworkInterfaceSecurityGroups = new ArrayList<>();
listSubNetworkInterfaceSecurityGroups.add("6727c950-9f01-47a2-a7aa-7d3686c4c95b");
CreateSubNetworkInterfaceOption subNetworkInterfacebody = new
CreateSubNetworkInterfaceOption();
subNetworkInterfacebody.withVirsubnetId("08278e6c-61ca-46c1-9fc3-0d4f6c12f193")
    .withParentId("637748df-2986-4350-8303-95d259580fb3")
    .withSecurityGroups(listSubNetworkInterfaceSecurityGroups);
body.withSubNetworkInterface(subNetworkInterfacebody);
request.withBody(body);
try {
    CreateSubNetworkInterfaceResponse response = client.createSubNetworkInterface(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

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.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.valueOf("<YOUR REGION>")) \
        .build()

    try:
        request = CreateSubNetworkInterfaceRequest()
        listSecurityGroupsSubNetworkInterface = [
```

```
        "6727c950-9f01-47a2-a7aa-7d3686c4c95b"
    ]
    subNetworkInterfacebody = CreateSubNetworkInterfaceOption(
        virsubnet_id="08278e6c-61ca-46c1-9fc3-0d4f6c12f193",
        parent_id="637748df-2986-4350-8303-95d259580fb3",
        security_groups=listSecurityGroupsSubNetworkInterface
    )
    request.body = CreateSubNetworkInterfaceRequestBody(
        sub_network_interface=subNetworkInterfacebody
    )
    response = client.create_sub_network_interface(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

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.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateSubNetworkInterfaceRequest{}
    var listSecurityGroupsSubNetworkInterface = []string{
        "6727c950-9f01-47a2-a7aa-7d3686c4c95b",
    }
    subNetworkInterfacebody := &model.CreateSubNetworkInterfaceOption{
        VirsubnetId: "08278e6c-61ca-46c1-9fc3-0d4f6c12f193",
        ParentId: "637748df-2986-4350-8303-95d259580fb3",
        SecurityGroups: &listSecurityGroupsSubNetworkInterface,
    }
    request.Body = &model.CreateSubNetworkInterfaceRequestBody{
        SubNetworkInterface: subNetworkInterfacebody,
    }
```

```
}  
response, err := client.CreateSubNetworkInterface(request)  
if err == nil {  
    fmt.Printf("%+v\n", response)  
} else {  
    fmt.Println(err)  
}  
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
201	Normal response to the POST operation. For more status codes, see Status Codes .

Error Codes

See [Error Codes](#).

5.5.2 Creating Supplementary Network Interfaces in Batches

Function

A supplementary network interface is a derivative resource based on an elastic network interface. You can use this API to create supplementary network interfaces in batches.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v3/{project_id}/vpc/sub-network-interfaces/batch-create

Table 5-117 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: ID of the project that a supplementary network interface belongs to. For details about how to obtain a project ID, see Obtaining a Project ID . Range: N/A

Request Parameters

Table 5-118 Request body parameters

Parameter	Mandatory	Type	Description
dry_run	No	Boolean	Definition: Whether to only check the request. Constraints: N/A Range: • true: A check request will be sent and no supplementary network interface will be created. Check items include mandatory parameters, request format, and constraints. If the check fails, an error will be returned. If the check succeeds, response code 202 will be returned. • false: A request will be sent and a supplementary network interface will be created. Default Value: false

Parameter	Mandatory	Type	Description
sub_network_interface	Yes	BatchCreateSubNetworkInterfaceOption object	Definition: Request body for creating a supplementary network interface. Constraints: N/A Range: N/A Default Value: N/A
count	Yes	Integer	Definition: Number of supplementary network interfaces to be created in batches. Constraints: N/A Range: N/A Default Value: N/A

Table 5-119 BatchCreateSubNetworkInterfaceOption

Parameter	Mandatory	Type	Description
virsubnet_id	Yes	String	Definition: ID of the virtual subnet that a supplementary network interface is located. Constraints: The value is in UUID format with hyphens (-). Range: N/A Default Value: N/A

Parameter	Mandatory	Type	Description
parent_id	Yes	String	Definition: ID of the elastic network interface that a supplementary network interface is attached to. Constraints: The value must be an existing elastic network interface ID. Range: N/A Default Value: N/A
security_groups	No	Array of strings	Definition: IDs of the security groups that a supplementary network interface is associated with. For example, "security_groups": ["a0608cbf-d047-4f54-8b28-cd7b59853fff"]. Constraints: If this parameter is not specified in the request, the supplementary network interface is automatically associated with the default security group after being created. Range: N/A Default Value: N/A

Parameter	Mandatory	Type	Description
description	No	String	Definition: Description of a supplementary network interface. Constraints: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >). Range: N/A Default Value: N/A
ipv6_enable	No	Boolean	Definition: Whether IPv6 is enabled for a supplementary network interface. Constraints: N/A Range: • true: IPv6 is enabled. • false: IPv6 is disabled. Default Value: false
project_id	No	String	Definition: ID of the project that a supplementary network interface belongs to. Constraints: This parameter can only be set to the tenant ID of the current tenant. If this parameter is not specified, the project ID of the current tenant is used by default. Range: N/A Default Value: N/A

Parameter	Mandatory	Type	Description
allowed_address_pairs	No	Array of AllowedAddressPair objects	Definition: IP/MAC address pair list of a supplementary network interface. For details, see the AllowedAddressPair object list. Constraints: • Configure a dedicated security group if a large CIDR block (subnet mask less than 24) is configured for parameter allowed_address_pairs. • In the hardware SDN networking plan, the ip_address attribute value cannot be in CIDR format. Range: N/A Default Value: N/A

Table 5-120 AllowedAddressPair

Parameter	Mandatory	Type	Description
ip_address	No	String	Definition: IP address. Constraints: Configure a dedicated security group if a large CIDR block (subnet mask less than 24) is configured for parameter allowed_address_pairs . Range: Single IP address, for example, 192.168.21.25 A CIDR block, for example, 192.168.21.0/24 Default Value: N/A

Parameter	Mandatory	Type	Description
mac_address	No	String	Definition: MAC address. Constraints: N/A Range: N/A Default Value: N/A

Response Parameters

Status code: 201

Table 5-121 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Request ID. Range: N/A
sub_network_inter faces	Array of SubNetworkInter face objects	Definition: Response body for creating supplementary network interfaces in batches. Range: N/A

Table 5-122 SubNetworkInterface

Parameter	Type	Description
id	String	Definition: ID of a supplementary network interface. After a supplementary network interface is created, a supplementary network interface ID is generated, which uniquely identifies the supplementary network interface. Range: The value is in UUID format with hyphens (-).
virsubnet_id	String	Definition: ID of the virtual subnet that a supplementary network interface is located. Range: The value is in UUID format with hyphens (-).
private_ip_address	String	Definition: Private IPv4 address of a supplementary network interface. Range: N/A
ipv6_ip_address	String	Definition: Private IPv6 address of a supplementary network interface. Range: N/A
mac_address	String	Definition: MAC address of a supplementary network interface. Range: The value is a valid MAC address assigned by the system randomly.
parent_device_id	String	Definition: Device ID of the host network interface that a supplementary network interface is attached to. Range: The value is in UUID format with hyphens (-).

Parameter	Type	Description
parent_id	String	Definition: ID of the elastic network interface that a supplementary network interface is attached to. Range: The value is in UUID format with hyphens (-).
description	String	Definition: Description of a supplementary network interface. Range: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >).
vpc_id	String	Definition: ID of the VPC that a supplementary network interface belongs to. Range: The value is in UUID format with hyphens (-).
vlan_id	Integer	Definition: VLAN ID of a supplementary network interface. Range: 1 to 4094
security_groups	Array of strings	Definition: IDs of the security groups that a supplementary network interface is associated with. For example, "security_groups": ["a0608cbf-d047-4f54-8b28-cd7b59853fff"]. Range: If this parameter is not specified in the request, the supplementary network interface is automatically associated with the default security group after being created.

Parameter	Type	Description
tags	Array of ResponseTag objects	Definition: Tags of a supplementary network interface, including tag keys and tag values, which can be used to classify and identify resources. For details, see the tag objects. Range: N/A
project_id	String	Definition: ID of the project that a supplementary network interface belongs to. Range: N/A
created_at	String	Definition: Time when a supplementary network interface was created. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .
allowed_address_pairs	Array of AllowedAddressPair objects	Definition: IP/MAC address pair list of a supplementary network interface. For details, see the AllowedAddressPair object list. Range: N/A
state	String	Definition: Status of a supplementary network interface. Range: • NORMAL: The supplementary network interface is attached to an elastic network interface. • UNBOUND: The supplementary network interface is not attached to an elastic network interface.

Parameter	Type	Description
instance_id	String	Definition: ID of the cloud service instance that a supplementary network interface is attached to, for example, RDS instance ID. Range: N/A
instance_type	String	Definition: Type of the cloud service instance that a supplementary network interface is attached to, for example, RDS. Range: N/A
scope	String	Definition: Public network egress information of the site where a supplementary network interface works. Range: • center: default value, indicating the central AZ. • <i>AZ ID:</i> a specific AZ
security_enabled	Boolean	Definition: Whether the security option is enabled for a supplementary network interface. If the option is not enabled, the security group does not take effect. Range: N/A

Table 5-123 ResponseTag

Parameter	Type	Description
key	String	Definition: Tag key. Range: • A tag key can contain a maximum of 128 Unicode characters and cannot be left blank. • Each tag key of a resource must be unique. • The value can contain: – Letters – Digits – Special characters: underscores (_), hyphens (-) – Chinese characters
value	String	Definition: Tag value. Range: • Each value can contain a maximum of 255 Unicode characters and can be left blank. • The value can contain: – Letters – Digits – Special characters: underscores (_), hyphens (-), periods (.) – Chinese characters

Table 5-124 AllowedAddressPair

Parameter	Type	Description
ip_address	String	Definition: IP address. Constraints: Configure a dedicated security group if a large CIDR block (subnet mask less than 24) is configured for parameter allowed_address_pairs . Range: Single IP address, for example, 192.168.21.25 A CIDR block, for example, 192.168.21.0/24 Default Value: N/A
mac_address	String	Definition: MAC address. Constraints: N/A Range: N/A Default Value: N/A

Example Requests

Create two 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": 2
}
```

Example Responses

Status code: 201

Normal response to the POST operation. For more status codes, see [Status Codes](#).

```
{
  "sub_network_interfaces": [ {
    "id": "4c2b455a-4c75-4c4d-bada-727be4d0f7b5",
    "project_id": "8c6fb137a48a428aaf9a0229dca4edb3",
    "vsubnet_id": "115b5a84-31dc-4b1e-8de9-bf5a75d2c566",
    "private_ip_address": "192.168.0.160",
    "ipv6_ip_address": null,
    "mac_address": "fa:16:3e:26:7e:1e",
    "parent_device_id": "285b2e45-2968-4f4c-8992-54e0d4c8da1d",
    "security_enabled": true,
    "security_groups": [ "6727c950-9f01-47a2-a7aa-7d3686c4c95b" ],
    "allowed_address_pairs": [ ],
    "vpc_id": "c10e1e02-9db2-4bd0-89ef-52536952627e",
    "instance_id": "",
    "instance_type": "",
    "description": "",
    "parent_id": "8b6c46f1-c68d-4bba-a922-2d97da185af5",
    "vlan_id": 3413,
    "state": "NORMAL",
    "tags": [ ],
    "scope": "center",
    "created_at": "2025-02-10T08:21:16Z"
  }, {
    "id": "a9ecbff0-d24f-493d-b62c-ee9b916db23a",
    "project_id": "8c6fb137a48a428aaf9a0229dca4edb3",
    "vsubnet_id": "115b5a84-31dc-4b1e-8de9-bf5a75d2c566",
    "private_ip_address": "192.168.0.20",
    "ipv6_ip_address": null,
    "mac_address": "fa:16:3e:26:7e:92",
    "parent_device_id": "285b2e45-2968-4f4c-8992-54e0d4c8da1d",
    "security_enabled": true,
    "security_groups": [ "6727c950-9f01-47a2-a7aa-7d3686c4c95b" ],
    "allowed_address_pairs": [ ],
    "vpc_id": "c10e1e02-9db2-4bd0-89ef-52536952627e",
    "instance_id": "",
    "instance_type": "",
    "description": "",
    "parent_id": "8b6c46f1-c68d-4bba-a922-2d97da185af5",
    "vlan_id": 595,
    "state": "NORMAL",
    "tags": [ ],
    "scope": "center",
    "created_at": "2025-02-10T08:21:16Z"
  } ],
  "request_id": "3f8a9620bea08c3e6ce0d4004d71f0c8"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Create two 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.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
```

```
import com.huaweicloud.sdk.vpc.v3.model.*;

import java.util.List;
import java.util.ArrayList;

public class BatchCreateSubNetworkInterfaceSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();

        BatchCreateSubNetworkInterfaceRequest request = new BatchCreateSubNetworkInterfaceRequest();
        BatchCreateSubNetworkInterfaceRequestBody body = new
        BatchCreateSubNetworkInterfaceRequestBody();
        List<String> listSubNetworkInterfaceSecurityGroups = new ArrayList<>();
        listSubNetworkInterfaceSecurityGroups.add("6727c950-9f01-47a2-a7aa-7d3686c4c95b");
        BatchCreateSubNetworkInterfaceOption subNetworkInterfacebody = new
        BatchCreateSubNetworkInterfaceOption();
        subNetworkInterfacebody.withVirsubnetId("115b5a84-31dc-4b1e-8de9-bf5a75d2c566")
            .withParentId("8b6c46f1-c68d-4bba-a922-2d97da185af5")
            .withSecurityGroups(listSubNetworkInterfaceSecurityGroups);
        body.withCount(2);
        body.withSubNetworkInterface(subNetworkInterfacebody);
        request.withBody(body);
        try {
            BatchCreateSubNetworkInterfaceResponse response =
            client.batchCreateSubNetworkInterface(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrMsg());
        }
    }
}
```

Python

Create two 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.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
```

```
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = BatchCreateSubNetworkInterfaceRequest()
        listSecurityGroupsSubNetworkInterface = [
            "6727c950-9f01-47a2-a7aa-7d3686c4c95b"
        ]
        subNetworkInterfacebody = BatchCreateSubNetworkInterfaceOption(
            virsubnet_id="115b5a84-31dc-4b1e-8de9-bf5a75d2c566",
            parent_id="8b6c46f1-c68d-4bba-a922-2d97da185af5",
            security_groups=listSecurityGroupsSubNetworkInterface
        )
        request.body = BatchCreateSubNetworkInterfaceRequestBody(
            count=2,
            sub_network_interface=subNetworkInterfacebody
        )
        response = client.batch_create_sub_network_interface(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Create two 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.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
```

```
projectId := "{project_id}"

auth := basic.NewCredentialsBuilder().
    WithAk(ak).
    WithSk(sk).
    WithProjectId(projectId).
    Build()

client := vpc.NewVpcClient(
    vpc.VpcClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.BatchCreateSubNetworkInterfaceRequest{}
var listSecurityGroupsSubNetworkInterface = []string{
    "6727c950-9f01-47a2-a7aa-7d3686c4c95b",
}
subNetworkInterfacebody := &model.BatchCreateSubNetworkInterfaceOption{
    VirsubnetId: "115b5a84-31dc-4b1e-8de9-bf5a75d2c566",
    ParentId: "8b6c46f1-c68d-4bba-a922-2d97da185af5",
    SecurityGroups: &listSecurityGroupsSubNetworkInterface,
}
request.Body = &model.BatchCreateSubNetworkInterfaceRequestBody{
    Count: int32(2),
    SubNetworkInterface: subNetworkInterfacebody,
}
response, err := client.BatchCreateSubNetworkInterface(request)
if err == nil {
    fmt.Printf("%v\n", response)
} else {
    fmt.Println(err)
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
201	Normal response to the POST operation. For more status codes, see Status Codes .

Error Codes

See [Error Codes](#).

5.5.3 Querying Supplementary Network Interfaces

Function

This API is used to query information about all supplementary network interfaces, including their IP addresses and VLAN IDs.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v3/{project_id}/vpc/sub-network-interfaces

Table 5-125 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: ID of the project that a supplementary network interface belongs to. For details about how to obtain a project ID, see Obtaining a Project ID . Range: N/A

Table 5-126 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Definition: Number of resources on each page. Range: 0 to 2000
marker	No	String	Definition: Start resource ID of pagination query. If the parameter is left blank, only resources on the first page are queried. Range: ID of a supplementary network interface.

Parameter	Mandatory	Type	Description
id	No	Array of strings	Definition: Supplementary network interface ID. You can use this field to filter supplementary network interfaces. Multiple IDs can be specified for filtering. Range: N/A
description	No	Array of strings	Definition: Description of a supplementary network interface. You can use this field to filter supplementary network interfaces. Multiple descriptions can be specified for filtering. Range: N/A
vpc_id	No	Array of strings	Definition: ID of the VPC that a supplementary network interface belongs to. You can use this field to filter supplementary network interfaces in one or more VPCs. Multiple VPC IDs can be specified for filtering. Range: N/A
virsubnet_id	No	Array of strings	Definition: ID of the virtual subnet that a supplementary network interface belongs to. You can use this field to filter supplementary network interfaces in one or more virtual subnets. Multiple virtual subnet IDs can be specified for filtering. Range: N/A

Parameter	Mandatory	Type	Description
parent_id	No	Array of strings	Definition: ID of the elastic network interface that a supplementary network interface is attached to. You can use this field to filter supplementary network interfaces attached to one or more elastic network interfaces. Multiple elastic network interface IDs can be specified for filtering. Range: N/A
private_ip_address	No	Array of strings	Definition: Private IPv4 address of a supplementary network interface. You can use this field to filter supplementary network interfaces. Multiple IP addresses can be specified for filtering. Range: N/A
mac_address	No	Array of strings	Definition: MAC address of a supplementary network interface. You can use this field to filter supplementary network interfaces. Multiple MAC addresses can be specified for filtering. Range: N/A
enable_eip	No	Boolean	Definition: Whether to filter a supplementary network interface with an EIP bound. You can use this field to filter supplementary network interfaces. Only one value can be specified for filtering. Range: true and false

Parameter	Mandatory	Type	Description
scope	No	String	Definition: Public network egress information of the site where a supplementary network interface works. You can use this field to filter supplementary network interfaces. Range: N/A
security_groups	No	Array of strings	Definition: ID of the security group that a supplementary network interface is associated with. You can use this field to filter supplementary network interfaces. Multiple IDs can be specified for filtering. Range: N/A
parent_device_id	No	Array of strings	Definition: Device ID of the host network interface that a supplementary network interface is attached to. You can use this field to filter supplementary network interfaces. Multiple IDs can be specified for filtering. Range: N/A
vlan_id	No	Array of integers	Definition: VLAN ID of a supplementary network interface. You can use this field to filter supplementary network interfaces. Multiple VLAN IDs can be specified for filtering. Range: 1 to 4094

Parameter	Mandatory	Type	Description
state	No	Array of strings	Definition: Status of a supplementary network interface. You can use this field to filter supplementary network interfaces. Multiple statuses can be specified for filtering. Range: NORMAL and UNBOUND
ipv6_ip_addresses	No	Array of strings	Definition: IPv6 address of a supplementary network interface. You can use this field to filter supplementary network interfaces. Multiple IP addresses can be specified for filtering. Range: N/A
instance_id	No	Array of strings	Definition: ID of the cloud service instance that a supplementary network interface is attached to, for example, RDS instance ID. You can use this field to filter supplementary network interfaces. Multiple IDs can be specified for filtering. Range: N/A
instance_type	No	Array of strings	Definition: Type of the cloud service instance that a supplementary network interface is attached to, for example, RDS. You can use this field to filter supplementary network interfaces. Multiple instance types can be specified for filtering. Range: N/A

Request Parameters

None

Response Parameters

Status code: 200

Table 5-127 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Request ID. Range: N/A
sub_network_inter faces	Array of SubNetworkInter face objects	Definition: Response body for querying supplementary network interfaces. Range: N/A
page_info	PageInfo object	Definition: Pagination information. Range: N/A

Table 5-128 SubNetworkInterface

Parameter	Type	Description
id	String	Definition: ID of a supplementary network interface. After a supplementary network interface is created, a supplementary network interface ID is generated, which uniquely identifies the supplementary network interface. Range: The value is in UUID format with hyphens (-).

Parameter	Type	Description
virsubnet_id	String	Definition: ID of the virtual subnet that a supplementary network interface is located. Range: The value is in UUID format with hyphens (-).
private_ip_address	String	Definition: Private IPv4 address of a supplementary network interface. Range: N/A
ipv6_ip_address	String	Definition: Private IPv6 address of a supplementary network interface. Range: N/A
mac_address	String	Definition: MAC address of a supplementary network interface. Range: The value is a valid MAC address assigned by the system randomly.
parent_device_id	String	Definition: Device ID of the host network interface that a supplementary network interface is attached to. Range: The value is in UUID format with hyphens (-).
parent_id	String	Definition: ID of the elastic network interface that a supplementary network interface is attached to. Range: The value is in UUID format with hyphens (-).

Parameter	Type	Description
description	String	Definition: Description of a supplementary network interface. Range: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >).
vpc_id	String	Definition: ID of the VPC that a supplementary network interface belongs to. Range: The value is in UUID format with hyphens (-).
vlan_id	Integer	Definition: VLAN ID of a supplementary network interface. Range: 1 to 4094
security_groups	Array of strings	Definition: IDs of the security groups that a supplementary network interface is associated with. For example, "security_groups": ["a0608cbf-d047-4f54-8b28-cd7b59853fff"]. Range: If this parameter is not specified in the request, the supplementary network interface is automatically associated with the default security group after being created.
tags	Array of ResponseTag objects	Definition: Tags of a supplementary network interface, including tag keys and tag values, which can be used to classify and identify resources. For details, see the tag objects. Range: N/A

Parameter	Type	Description
project_id	String	Definition: ID of the project that a supplementary network interface belongs to. Range: N/A
created_at	String	Definition: Time when a supplementary network interface was created. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .
allowed_address_pairs	Array of AllowedAddressPair objects	Definition: IP/MAC address pair list of a supplementary network interface. For details, see the AllowedAddressPair object list. Range: N/A
state	String	Definition: Status of a supplementary network interface. Range: • NORMAL: The supplementary network interface is attached to an elastic network interface. • UNBOUND: The supplementary network interface is not attached to an elastic network interface.
instance_id	String	Definition: ID of the cloud service instance that a supplementary network interface is attached to, for example, RDS instance ID. Range: N/A
instance_type	String	Definition: Type of the cloud service instance that a supplementary network interface is attached to, for example, RDS. Range: N/A

Parameter	Type	Description
scope	String	Definition: Public network egress information of the site where a supplementary network interface works. Range: • center: default value, indicating the central AZ. • AZ ID: a specific AZ
security_enabled	Boolean	Definition: Whether the security option is enabled for a supplementary network interface. If the option is not enabled, the security group does not take effect. Range: N/A

Table 5-129 ResponseTag

Parameter	Type	Description
key	String	Definition: Tag key. Range: • A tag key can contain a maximum of 128 Unicode characters and cannot be left blank. • Each tag key of a resource must be unique. • The value can contain: – Letters – Digits – Special characters: underscores (_), hyphens (-) – Chinese characters

Parameter	Type	Description
value	String	Definition: Tag value. Range: - Each value can contain a maximum of 255 Unicode characters and can be left blank. - The value can contain: - Letters - Digits - Special characters: underscores (_), hyphens (-), periods (.) - Chinese characters

Table 5-130 AllowedAddressPair

Parameter	Type	Description
ip_address	String	Definition: IP address. Constraints: Configure a dedicated security group if a large CIDR block (subnet mask less than 24) is configured for parameter allowed_address_pairs . Range: Single IP address, for example, 192.168.21.25 A CIDR block, for example, 192.168.21.0/24 Default Value: N/A
mac_address	String	Definition: MAC address. Constraints: N/A Range: N/A Default Value: N/A

Table 5-131 PageInfo

Parameter	Type	Description
previous_marker	String	Definition: The first record on the current page. Range: N/A
current_count	Integer	Definition: Total number of resources on the current page. Range: N/A
next_marker	String	Definition: The last record on the current page. The next_marker field does not exist if the page is the last one. Range: N/A

Example Requests

- Querying supplementary network interfaces by its ID
GET https://{Endpoint}/v3/8c6fb137a48a428aaf9a0229dca4edb3/vpc/sub-network-interfaces?id=022b5c53-20e1-4f4b-b90c-0575a5e97412&id=056d6cb4-b436-460d-9a63-67666bf3ea9c
- Querying supplementary network interfaces by combined filters
https://{Endpoint}/v3/8c6fb137a48a428aaf9a0229dca4edb3/vpc/sub-network-interfaces?virsubnet_id=3eae2c96-de45-4c41-bf2d-e4ad53a2acb4&private_ip_address=192.168.22.177&parent_id=5eb9dc59-8159-4197-88ea-f3507ad8e0a7
- Querying supplementary network interfaces by page
GET https://{Endpoint}/v3/8c6fb137a48a428aaf9a0229dca4edb3/vpc/sub-network-interfaces?limit=2

Example Responses

Status code: 200

Normal response to the GET operation. For more status codes, see [Status Codes](#).

```
{
  "request_id" : "db2bd86cad7519610d9d405228e63076",
  "sub_network_interfaces" : [ {
    "id" : "022b5c53-20e1-4f4b-b90c-0575a5e97412",
    "project_id" : "8c6fb137a48a428aaf9a0229dca4edb3",
    "virsubnet_id" : "3c15c3b0-0df4-4115-9c18-e67a8a0d7702",
    "private_ip_address" : "192.168.0.160",
    "ipv6_ip_address" : null,
    "mac_address" : "fa:16:3e:26:7e:1e",
    "parent_device_id" : "285b2e45-2968-4f4c-8992-54e0d4c8da1d",
    "security_enabled" : false,
    "security_groups" : [ ],
    "allowed_address_pairs" : [ ],
```

```
"vpc_id" : "c10e1e02-9db2-4bd0-89ef-52536952627e",
"instance_id" : "",
"instance_type" : "",
"description" : "",
"parent_id" : "00336617-4552-48c5-9856-f539f4e9aca2",
"vlan_id" : 3413,
"state" : null,
"tags" : [ ],
"scope" : "center",
"created_at" : "2025-02-10T08:21:16Z"
}, {
  "id" : "056d6cb4-b436-460d-9a63-67666bf3ea9c",
  "project_id" : "8c6fb137a48a428aaf9a0229dca4edb3",
  "vsubnet_id" : "3c15c3b0-0df4-4115-9c18-e67a8a0d7702",
  "private_ip_address" : "192.168.0.20",
  "ipv6_ip_address" : null,
  "mac_address" : "fa:16:3e:26:7e:92",
  "parent_device_id" : "285b2e45-2968-4f4c-8992-54e0d4c8da1d",
  "security_enabled" : false,
  "security_groups" : [ ],
  "allowed_address_pairs" : [ ],
  "vpc_id" : "c10e1e02-9db2-4bd0-89ef-52536952627e",
  "instance_id" : "",
  "instance_type" : "",
  "description" : "",
  "parent_id" : "00336617-4552-48c5-9856-f539f4e9aca2",
  "vlan_id" : 595,
  "state" : null,
  "tags" : [ ],
  "scope" : "center",
  "created_at" : "2025-02-10T08:21:16Z"
}],
"page_info" : {
  "previous_marker" : "4c2b455a-4c75-4c4d-bada-727be4d0f7b5",
  "current_count" : 2
}
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class ListSubNetworkInterfacesSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";
```

```
ICredential auth = new BasicCredentials()
    .withProjectId(projectId)
    .withAk(ak)
    .withSk(sk);

VpcClient client = VpcClient.newBuilder()
    .withCredential(auth)
    .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
    .build();
ListSubNetworkInterfacesRequest request = new ListSubNetworkInterfacesRequest();
try {
    ListSubNetworkInterfacesResponse response = client.listSubNetworkInterfaces(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListSubNetworkInterfacesRequest()
        response = client.list_sub_network_interfaces(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
```

```
"fmt"
"github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
"github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListSubNetworkInterfacesRequest{}
    response, err := client.ListSubNetworkInterfaces(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Normal response to the GET operation. For more status codes, see Status Codes .

Error Codes

See [Error Codes](#).

5.5.4 Querying the Details of a Supplementary Network Interface

Function

This API is used to query information about a supplementary network interface, including the IP address and VLAN ID.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v3/{project_id}/vpc/sub-network-interfaces/{sub_network_interface_id}

Table 5-132 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: ID of the project that a supplementary network interface belongs to. For details about how to obtain a project ID, see Obtaining a Project ID . Range: N/A
sub_network_interface_id	Yes	String	Definition: ID of a supplementary network interface. Range: N/A

Request Parameters

None

Response Parameters

Status code: 200

Table 5-133 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Request ID. Range: N/A
sub_network_interface	SubNetworkInterface object	Definition: Response body for querying details about a supplementary network interface. Range: N/A

Table 5-134 SubNetworkInterface

Parameter	Type	Description
id	String	Definition: ID of a supplementary network interface. After a supplementary network interface is created, a supplementary network interface ID is generated, which uniquely identifies the supplementary network interface. Range: The value is in UUID format with hyphens (-).
virsubnet_id	String	Definition: ID of the virtual subnet that a supplementary network interface is located. Range: The value is in UUID format with hyphens (-).
private_ip_address	String	Definition: Private IPv4 address of a supplementary network interface. Range: N/A

Parameter	Type	Description
ipv6_ip_address	String	Definition: Private IPv6 address of a supplementary network interface. Range: N/A
mac_address	String	Definition: MAC address of a supplementary network interface. Range: The value is a valid MAC address assigned by the system randomly.
parent_device_id	String	Definition: Device ID of the host network interface that a supplementary network interface is attached to. Range: The value is in UUID format with hyphens (-).
parent_id	String	Definition: ID of the elastic network interface that a supplementary network interface is attached to. Range: The value is in UUID format with hyphens (-).
description	String	Definition: Description of a supplementary network interface. Range: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >).
vpc_id	String	Definition: ID of the VPC that a supplementary network interface belongs to. Range: The value is in UUID format with hyphens (-).

Parameter	Type	Description
vlan_id	Integer	Definition: VLAN ID of a supplementary network interface. Range: 1 to 4094
security_groups	Array of strings	Definition: IDs of the security groups that a supplementary network interface is associated with. For example, "security_groups": ["a0608cbf-d047-4f54-8b28-cd7b59853fff"]. Range: If this parameter is not specified in the request, the supplementary network interface is automatically associated with the default security group after being created.
tags	Array of ResponseTag objects	Definition: Tags of a supplementary network interface, including tag keys and tag values, which can be used to classify and identify resources. For details, see the tag objects. Range: N/A
project_id	String	Definition: ID of the project that a supplementary network interface belongs to. Range: N/A
created_at	String	Definition: Time when a supplementary network interface was created. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .

Parameter	Type	Description
allowed_address_pairs	Array of AllowedAddressPair objects	Definition: IP/MAC address pair list of a supplementary network interface. For details, see the AllowedAddressPair object list. Range: N/A
state	String	Definition: Status of a supplementary network interface. Range: • NORMAL: The supplementary network interface is attached to an elastic network interface. • UNBOUND: The supplementary network interface is not attached to an elastic network interface.
instance_id	String	Definition: ID of the cloud service instance that a supplementary network interface is attached to, for example, RDS instance ID. Range: N/A
instance_type	String	Definition: Type of the cloud service instance that a supplementary network interface is attached to, for example, RDS. Range: N/A
scope	String	Definition: Public network egress information of the site where a supplementary network interface works. Range: • center: default value, indicating the central AZ. • AZ ID: a specific AZ

Parameter	Type	Description
security_enabled	Boolean	Definition: Whether the security option is enabled for a supplementary network interface. If the option is not enabled, the security group does not take effect. Range: N/A

Table 5-135 ResponseTag

Parameter	Type	Description
key	String	Definition: Tag key. Range: • A tag key can contain a maximum of 128 Unicode characters and cannot be left blank. • Each tag key of a resource must be unique. • The value can contain: – Letters – Digits – Special characters: underscores (_), hyphens (-) – Chinese characters
value	String	Definition: Tag value. Range: • Each value can contain a maximum of 255 Unicode characters and can be left blank. • The value can contain: – Letters – Digits – Special characters: underscores (_), hyphens (-), periods (.) – Chinese characters

Table 5-136 AllowedAddressPair

Parameter	Type	Description
ip_address	String	Definition: IP address. Constraints: Configure a dedicated security group if a large CIDR block (subnet mask less than 24) is configured for parameter allowed_address_pairs . Range: Single IP address, for example, 192.168.21.25 A CIDR block, for example, 192.168.21.0/24 Default Value: N/A
mac_address	String	Definition: MAC address. Constraints: N/A Range: N/A Default Value: N/A

Example Requests

Query the details of the supplementary network interfaces whose ID is **2be868f2-f7c9-48db-abc0-eea0b9105b0**.

GET https://{Endpoint}/v3/8c6fb137a48a428aaf9a0229dca4edb3/vpc/sub-network-interfaces/2be868f2-f7c9-48db-abc0-eea0b9105b0d

Example Responses

Status code: 200

Normal response to the GET operation. For more status codes, see [Status Codes](#).

```
{
  "sub_network_interface" : {
    "id" : "2be868f2-f7c9-48db-abc0-eea0b9105b0d",
    "project_id" : "8c6fb137a48a428aaf9a0229dca4edb3",
    "virsubnet_id" : "3c15c3b0-0df4-4115-9c18-e67a8a0d7702",
    "private_ip_address" : "192.168.0.160",
    "ipv6_ip_address" : null,
    "mac_address" : "fa:16:3e:26:7e:1e",
    "parent_device_id" : "285b2e45-2968-4f4c-8992-54e0d4c8da1d",
```

```
"security_enabled" : false,
"security_groups" : [ ],
"allowed_address_pairs" : [ ],
"vpc_id" : "c10e1e02-9db2-4bd0-89ef-52536952627e",
"instance_id" : "",
"instance_type" : "",
"description" : "",
"parent_id" : "00336617-4552-48c5-9856-f539f4e9aca2",
"vlan_id" : 3413,
"state" : null,
"tags" : [ ],
"scope" : "center",
"created_at" : "2025-02-10T08:21:16Z"
},
"request_id" : "16fe2bcb91bd7ad03a895adbc63bf44e"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class ShowSubNetworkInterfaceSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();
        ShowSubNetworkInterfaceRequest request = new ShowSubNetworkInterfaceRequest();
        request.withSubNetworkInterfaceId("{sub_network_interface_id}");
        try {
            ShowSubNetworkInterfaceResponse response = client.showSubNetworkInterface(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getStatusCode());
        }
    }
}
```

```
        System.out.println(e.getRequestId());
        System.out.println(e.getErrorCode());
        System.out.println(e.getErrorMsg());
    }
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowSubNetworkInterfaceRequest()
        request.sub_network_interface_id = "{sub_network_interface_id}"
        response = client.show_sub_network_interface(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
```

```
WithSk(sk).
WithProjectId(projectId).
Build()

client := vpc.NewVpcClient(
    vpc.VpcClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.ShowSubNetworkInterfaceRequest{}
request.SubNetworkInterfaceId = "{sub_network_interface_id}"
response, err := client.ShowSubNetworkInterface(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Normal response to the GET operation. For more status codes, see Status Codes .

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 of a tenant.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v3/{project_id}/vpc/sub-network-interfaces/count

Table 5-137 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: ID of the project that a supplementary network interface belongs to. For details about how to obtain a project ID, see Obtaining a Project ID . Range: N/A

Request Parameters

None

Response Parameters

Status code: 200

Table 5-138 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Request ID. Range: N/A
sub_network_interfaces	Integer	Definition: Number of supplementary network interfaces. Range: N/A

Example Requests

Querying the number of supplementary network interfaces

GET https://{Endpoint}/v3/8c6fb137a48a428aaf9a0229dca4edb3/vpc/sub-network-interfaces/count

Example Responses

Status code: 200

Normal response to the GET operation. For more status codes, see [Status Codes](#).

```
{
  "sub_network_interfaces" : 2,
  "request_id" : "4a79f1f7-67eb-43be-a8be-eb57ba894f90"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class ShowSubNetworkInterfacesQuantitySolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();
        ShowSubNetworkInterfacesQuantityRequest request = new
        ShowSubNetworkInterfacesQuantityRequest();
        try {
            ShowSubNetworkInterfacesQuantityResponse response =
            client.showSubNetworkInterfacesQuantity(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8
```

```
import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowSubNetworkInterfacesQuantityRequest()
        response = client.show_sub_network_interfaces_quantity(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowSubNetworkInterfacesQuantityRequest{}
    response, err := client.ShowSubNetworkInterfacesQuantity(request)
```

```
if err == nil {  
    fmt.Printf("%+v\n", response)  
} else {  
    fmt.Println(err)  
}  
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Normal response to the GET operation. For more status codes, see Status Codes .

Error Codes

See [Error Codes](#).

5.5.6 Updating a Supplementary Network Interface

Function

This API is used to update the basic information about a supplementary network interface, such as the associated security group and description.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v3/{project_id}/vpc/sub-network-interfaces/{sub_network_interface_id}

Table 5-139 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: ID of the project that a supplementary network interface belongs to. For details about how to obtain a project ID, see Obtaining a Project ID . Range: N/A
sub_network_interface_id	Yes	String	Definition: ID of a supplementary network interface. Range: N/A

Request Parameters

Table 5-140 Request body parameters

Parameter	Mandatory	Type	Description
dry_run	No	Boolean	Definition: Whether to only check the request. Constraints: N/A Range: • true: A check request will be sent and the supplementary network interface will not be updated. Check items include mandatory parameters, request format, and constraints. If the check fails, an error will be returned. If the check succeeds, response code 202 will be returned. • false: A request will be sent and the supplementary network interface will be updated. Default Value: false
sub_network_interface	Yes	UpdateSubNetworkInterfaceOption object	Definition: Request body for updating a supplementary network interface. Constraints: N/A Range: N/A Default Value: N/A

Table 5-141 UpdateSubNetworkInterfaceOption

Parameter	Mandatory	Type	Description
description	No	String	Definition: Description of a supplementary network interface. Constraints: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >). Range: N/A Default Value: N/A
security_groups	No	Array of strings	Definition: IDs of the security groups that a supplementary network interface is associated with. For example, "security_groups": ["a0608cbf-d047-4f54-8b28-cd7b59853fff"]. Constraints: N/A Range: N/A Default Value: N/A

Parameter	Mandatory	Type	Description
allowed_address_pairs	No	Array of AllowedAddressPair objects	Definition: IP/MAC address pair list of a supplementary network interface. For details, see the AllowedAddressPair object list. Constraints: - Configure a dedicated security group if a large CIDR block (subnet mask less than 24) is configured for parameter allowed_address_pairs. - In the hardware SDN networking plan, the ip_address attribute value cannot be in CIDR format. Range: N/A Default Value: N/A

Table 5-142 AllowedAddressPair

Parameter	Mandatory	Type	Description
ip_address	No	String	Definition: IP address. Constraints: Configure a dedicated security group if a large CIDR block (subnet mask less than 24) is configured for parameter allowed_address_pairs . Range: Single IP address, for example, 192.168.21.25 A CIDR block, for example, 192.168.21.0/24 Default Value: N/A

Parameter	Mandatory	Type	Description
mac_address	No	String	Definition: MAC address. Constraints: N/A Range: N/A Default Value: N/A

Response Parameters

Status code: 200

Table 5-143 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Request ID. Range: N/A
sub_network_interface	SubNetworkInterface object	Definition: Response body for updating a supplementary network interface. Range: N/A

Table 5-144 SubNetworkInterface

Parameter	Type	Description
id	String	Definition: ID of a supplementary network interface. After a supplementary network interface is created, a supplementary network interface ID is generated, which uniquely identifies the supplementary network interface. Range: The value is in UUID format with hyphens (-).

Parameter	Type	Description
virsubnet_id	String	Definition: ID of the virtual subnet that a supplementary network interface is located. Range: The value is in UUID format with hyphens (-).
private_ip_address	String	Definition: Private IPv4 address of a supplementary network interface. Range: N/A
ipv6_ip_address	String	Definition: Private IPv6 address of a supplementary network interface. Range: N/A
mac_address	String	Definition: MAC address of a supplementary network interface. Range: The value is a valid MAC address assigned by the system randomly.
parent_device_id	String	Definition: Device ID of the host network interface that a supplementary network interface is attached to. Range: The value is in UUID format with hyphens (-).
parent_id	String	Definition: ID of the elastic network interface that a supplementary network interface is attached to. Range: The value is in UUID format with hyphens (-).

Parameter	Type	Description
description	String	Definition: Description of a supplementary network interface. Range: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >).
vpc_id	String	Definition: ID of the VPC that a supplementary network interface belongs to. Range: The value is in UUID format with hyphens (-).
vlan_id	Integer	Definition: VLAN ID of a supplementary network interface. Range: 1 to 4094
security_groups	Array of strings	Definition: IDs of the security groups that a supplementary network interface is associated with. For example, "security_groups": ["a0608cbf-d047-4f54-8b28-cd7b59853fff"]. Range: If this parameter is not specified in the request, the supplementary network interface is automatically associated with the default security group after being created.
tags	Array of ResponseTag objects	Definition: Tags of a supplementary network interface, including tag keys and tag values, which can be used to classify and identify resources. For details, see the tag objects. Range: N/A

Parameter	Type	Description
project_id	String	Definition: ID of the project that a supplementary network interface belongs to. Range: N/A
created_at	String	Definition: Time when a supplementary network interface was created. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .
allowed_address_pairs	Array of AllowedAddressPair objects	Definition: IP/MAC address pair list of a supplementary network interface. For details, see the AllowedAddressPair object list. Range: N/A
state	String	Definition: Status of a supplementary network interface. Range: • NORMAL: The supplementary network interface is attached to an elastic network interface. • UNBOUND: The supplementary network interface is not attached to an elastic network interface.
instance_id	String	Definition: ID of the cloud service instance that a supplementary network interface is attached to, for example, RDS instance ID. Range: N/A
instance_type	String	Definition: Type of the cloud service instance that a supplementary network interface is attached to, for example, RDS. Range: N/A

Parameter	Type	Description
scope	String	Definition: Public network egress information of the site where a supplementary network interface works. Range: • center: default value, indicating the central AZ. • AZ ID: a specific AZ
security_enabled	Boolean	Definition: Whether the security option is enabled for a supplementary network interface. If the option is not enabled, the security group does not take effect. Range: N/A

Table 5-145 ResponseTag

Parameter	Type	Description
key	String	Definition: Tag key. Range: • A tag key can contain a maximum of 128 Unicode characters and cannot be left blank. • Each tag key of a resource must be unique. • The value can contain: – Letters – Digits – Special characters: underscores (_), hyphens (-) – Chinese characters

Parameter	Type	Description
value	String	Definition: Tag value. Range: - Each value can contain a maximum of 255 Unicode characters and can be left blank. - The value can contain: - Letters - Digits - Special characters: underscores (_), hyphens (-), periods (.) - Chinese characters

Table 5-146 AllowedAddressPair

Parameter	Type	Description
ip_address	String	Definition: IP address. Constraints: Configure a dedicated security group if a large CIDR block (subnet mask less than 24) is configured for parameter allowed_address_pairs . Range: Single IP address, for example, 192.168.21.25 A CIDR block, for example, 192.168.21.0/24 Default Value: N/A
mac_address	String	Definition: MAC address. Constraints: N/A Range: N/A Default Value: N/A

Example Requests

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" ],
    "allowed_address_pairs": [ {
      "ip_address": "1.1.1.1/0"
    } ]
  }
}
```

Example Responses

Status code: 200

Normal response to the PUT operation. For more status codes, see [Status Codes](#).

```
{
  "sub_network_interface": {
    "id": "2be868f2-f7c9-48db-abc0-eea0b9105b0d",
    "project_id": "6b32266bde64091a138e9ec19cff361",
    "virsubnet_id": "3c15c3b0-0df4-4115-9c18-e67a8a0d7702",
    "private_ip_address": "192.168.0.160",
    "ipv6_ip_address": null,
    "mac_address": "fa:16:3e:26:7e:1e",
    "parent_device_id": "285b2e45-2968-4f4c-8992-54e0d4c8da1d",
    "security_enabled": false,
    "security_groups": [ "6727c950-9f01-47a2-a7aa-7d3686c4c95b" ],
    "allowed_address_pairs": [ {
      "ip_address": "1.1.1.1/0",
      "mac_address": "fa:16:3e:26:7e:1e"
    } ],
    "vpc_id": "c10e1e02-9db2-4bd0-89ef-52536952627e",
    "instance_id": "",
    "instance_type": "",
    "description": "aaa",
    "parent_id": "00336617-4552-48c5-9856-f539f4e9aca2",
    "vlan_id": 3413,
    "state": null,
    "tags": [ ],
    "scope": "center",
    "created_at": "2025-02-10T08:21:16Z"
  },
  "request_id": "d346a69661d82c7b14bdc7ac0cd62cbd"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Change the security group that is associated with the supplementary network interface whose ID is **2be868f2-f7c9-48db-abc0-eea0b9105b0d**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
```

```
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

import java.util.List;
import java.util.ArrayList;

public class UpdateSubNetworkInterfaceSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();

        UpdateSubNetworkInterfaceRequest request = new UpdateSubNetworkInterfaceRequest();
        request.withSubNetworkInterfaceId("{sub_network_interface_id}");
        UpdateSubNetworkInterfaceRequestBody body = new UpdateSubNetworkInterfaceRequestBody();
        List<AllowedAddressPair> listSubNetworkInterfaceAllowedAddressPairs = new ArrayList<>();
        listSubNetworkInterfaceAllowedAddressPairs.add(
            new AllowedAddressPair()
                .withIpAddress("1.1.1.1/0")
        );
        List<String> listSubNetworkInterfaceSecurityGroups = new ArrayList<>();
        listSubNetworkInterfaceSecurityGroups.add("6727c950-9f01-47a2-a7aa-7d3686c4c95b");
        UpdateSubNetworkInterfaceOption subNetworkInterfacebody = new
        UpdateSubNetworkInterfaceOption();
        subNetworkInterfacebody.withSecurityGroups(listSubNetworkInterfaceSecurityGroups)
            .withAllowedAddressPairs(listSubNetworkInterfaceAllowedAddressPairs);
        body.withSubNetworkInterface(subNetworkInterfacebody);
        request.withBody(body);
        try {
            UpdateSubNetworkInterfaceResponse response = client.updateSubNetworkInterface(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Change the security group that is associated with the supplementary network interface whose ID is **2be868f2-f7c9-48db-abc0-eea0b9105b0d**.


```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdateSubNetworkInterfaceRequest()
        request.sub_network_interface_id = "{sub_network_interface_id}"
        listAllowedAddressPairsSubNetworkInterface = [
            AllowedAddressPair(
                ip_address="1.1.1.1/0"
            )
        ]
        listSecurityGroupsSubNetworkInterface = [
            "6727c950-9f01-47a2-a7aa-7d3686c4c95b"
        ]
        subNetworkInterfacebody = UpdateSubNetworkInterfaceOption(
            security_groups=listSecurityGroupsSubNetworkInterface,
            allowed_address_pairs=listAllowedAddressPairsSubNetworkInterface
        )
        request.body = UpdateSubNetworkInterfaceRequestBody(
            sub_network_interface=subNetworkInterfacebody
        )
        response = client.update_sub_network_interface(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Change the security group that is associated with the supplementary network interface whose ID is **2be868f2-f7c9-48db-abc0-eea0b9105b0d**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
```

```
variables and decrypted during use to ensure security.
// In this example, AK and SK are stored in environment variables for authentication. Before running this
example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak := os.Getenv("CLOUD_SDK_AK")
sk := os.Getenv("CLOUD_SDK_SK")
projectId := "{project_id}"

auth := basic.NewCredentialsBuilder().
    WithAk(ak).
    WithSk(sk).
    WithProjectId(projectId).
    Build()

client := vpc.NewVpcClient(
    vpc.VpcClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.UpdateSubNetworkInterfaceRequest{}
request.SubNetworkInterfaceId = "{sub_network_interface_id}"
ipAddressAllowedAddressPairs := "1.1.1.1/0"
var listAllowedAddressPairsSubNetworkInterface = []model.AllowedAddressPair{
    {
        IpAddress: &ipAddressAllowedAddressPairs,
    },
}
var listSecurityGroupsSubNetworkInterface = []string{
    "6727c950-9f01-47a2-a7aa-7d3686c4c95b",
}
subNetworkInterfacebody := &model.UpdateSubNetworkInterfaceOption{
    SecurityGroups: &listSecurityGroupsSubNetworkInterface,
    AllowedAddressPairs: &listAllowedAddressPairsSubNetworkInterface,
}
request.Body = &model.UpdateSubNetworkInterfaceRequestBody{
    SubNetworkInterface: subNetworkInterfacebody,
}
response, err := client.UpdateSubNetworkInterface(request)
if err == nil {
    fmt.Printf("%v\n", response)
} else {
    fmt.Println(err)
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Normal response to the PUT operation. For more status codes, see Status Codes .

Error Codes

See [Error Codes](#).

5.5.7 Deleting a Supplementary Network Interface

Function

This API is used to delete a supplementary network interface that is no longer required.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v3/{project_id}/vpc/sub-network-interfaces/{sub_network_interface_id}

Table 5-147 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: ID of the project that a supplementary network interface belongs to. For details about how to obtain a project ID, see Obtaining a Project ID . Range: N/A
sub_network_interface_id	Yes	String	Definition: ID of a supplementary network interface. Range: N/A

Request Parameters

None

Response Parameters

Status code: 204

Normal response to the DELETE operation. For more status codes, see [Status Codes](#).

None

Example Requests

Delete the supplementary network interfaces whose ID is **2be868f2-f7c9-48db-abc0-eea0b9105b0**.

```
DELETE https://{Endpoint}/v3/8c6fb137a48a428aaf9a0229dca4edb3/vpc/sub-network-interfaces/2be868f2-f7c9-48db-abc0-eea0b9105b0d
```

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class DeleteSubNetworkInterfaceSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();
        DeleteSubNetworkInterfaceRequest request = new DeleteSubNetworkInterfaceRequest();
        request.withSubNetworkInterfaceId("{sub_network_interface_id}");
        try {
            DeleteSubNetworkInterfaceResponse response = client.deleteSubNetworkInterface(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

```
    }  
  }  
}
```

Python

```
# coding: utf-8  
  
import os  
from huaweicloudsdkcore.auth.credentials import BasicCredentials  
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion  
from huaweicloudsdkcore.exceptions import exceptions  
from huaweicloudsdkvpc.v3 import *  
  
if __name__ == "__main__":  
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security  
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment  
    # variables and decrypted during use to ensure security.  
    # In this example, AK and SK are stored in environment variables for authentication. Before running this  
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak = os.environ["CLOUD_SDK_AK"]  
    sk = os.environ["CLOUD_SDK_SK"]  
    projectId = "{project_id}"  
  
    credentials = BasicCredentials(ak, sk, projectId)  
  
    client = VpcClient.new_builder() \  
        .with_credentials(credentials) \  
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \  
        .build()  
  
    try:  
        request = DeleteSubNetworkInterfaceRequest()  
        request.sub_network_interface_id = "{sub_network_interface_id}"  
        response = client.delete_sub_network_interface(request)  
        print(response)  
    except exceptions.ClientRequestException as e:  
        print(e.status_code)  
        print(e.request_id)  
        print(e.error_code)  
        print(e.error_msg)
```

Go

```
package main  
  
import (  
    "fmt"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"  
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"  
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"  
)  
  
func main() {  
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security  
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment  
    // variables and decrypted during use to ensure security.  
    // In this example, AK and SK are stored in environment variables for authentication. Before running this  
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak := os.Getenv("CLOUD_SDK_AK")  
    sk := os.Getenv("CLOUD_SDK_SK")  
    projectId := "{project_id}"  
  
    auth := basic.NewCredentialsBuilder().  
        WithAk(ak).  
        WithSk(sk).  
        WithProjectId(projectId).  
        Build()
```

```
client := vpc.NewVpcClient(  
    vpc.VpcClientBuilder().  
        WithRegion(region.ValueOf("<YOUR REGION>")).  
        WithCredential(auth).  
        Build())  
  
request := &model.DeleteSubNetworkInterfaceRequest{  
    request.SubNetworkInterfaceId = "{sub_network_interface_id}"  
    response, err := client.DeleteSubNetworkInterface(request)  
    if err == nil {  
        fmt.Printf("%+v\n", response)  
    } else {  
        fmt.Println(err)  
    }  
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
204	Normal response to the DELETE operation. For more status codes, see Status Codes .

Error Codes

See [Error Codes](#).

5.6 Traffic Mirror Sessions

5.6.1 Querying Traffic Mirror Sessions

Function

This API is used to query information about all traffic mirror sessions, including the name and type.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v3/{project_id}/vpc/traffic-mirror-sessions

Table 5-148 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: ID of the project that a traffic mirror session belongs to. For details about how to obtain a project ID, see Obtaining a Project ID . Range: N/A

Table 5-149 Query Parameters

Parameter	Mandatory	Type	Description
id	No	Array of strings	Definition: ID of a traffic mirror session. You can use this field to accurately filter traffic mirror sessions. Multiple IDs can be specified for filtering. Range: N/A
name	No	Array of strings	Definition: Name of a traffic mirror session. You can use this field to filter traffic mirror sessions. Multiple names can be specified for filtering. Range: N/A
description	No	Array of strings	Definition: Description of a traffic mirror session. You can use this field to filter traffic mirror sessions. Multiple descriptions can be specified for filtering. Range: N/A

Parameter	Mandatory	Type	Description
enabled	No	Boolean	Definition: Whether a traffic mirror session is enabled. You can use this field to filter traffic mirror sessions. Only one value can be specified for filtering. Range: • true: Filter traffic mirror sessions that are enabled. • false: Filter traffic mirror sessions that are disabled.
packet_length	No	Array of integers	Definition: Packet length of a traffic mirror session. You can use this field to filter traffic mirror sessions. Multiple packet lengths can be specified for filtering. Range: 1 to 1460
priority	No	Array of integers	Definition: Priority of a traffic mirror session. You can use this field to filter traffic mirror sessions. Multiple priorities can be specified for filtering. Range: 1 to 32766
traffic_mirror_filter_id	No	Array of strings	Definition: ID of the traffic mirror filter associated with a traffic mirror session. You can use this field to filter traffic mirror sessions. Multiple IDs can be specified for filtering. Range: N/A

Parameter	Mandatory	Type	Description
traffic_mirror_target_type	No	Array of strings	Definition: Type of the traffic mirror target associated with a traffic mirror session. You can use this field to filter traffic mirror sessions. Multiple types can be specified for filtering. Range: • eni: The mirror target is an elastic network interface. • elb: The mirror target is a private network load balancer.
traffic_mirror_target_id	No	Array of strings	Definition: ID of the traffic mirror target associated with a traffic mirror session. You can use this field to filter traffic mirror sessions. Multiple IDs can be specified for filtering. Range: N/A
type	No	Array of strings	Definition: Type of the traffic mirror source associated with a traffic mirror session. You can use this field to filter traffic mirror sessions. Multiple types can be specified for filtering. Range: • eni: elastic network interface • eip: EIP
virtual_network_id	No	Array of integers	Definition: VXLAN network identifier (VNI) of a traffic mirror session. You can use this field to filter traffic mirror sessions. Multiple VNIs can be specified for filtering. Range: 0 to 16777215

Request Parameters

None

Response Parameters

Status code: 200

Table 5-150 Response body parameters

Parameter	Type	Description
traffic_mirror_sessions	Array of TrafficMirrorSession objects	Definition: Response body for querying traffic mirror sessions. Range: N/A
page_info	PageInfo object	Definition: Pagination information. Range: N/A
request_id	String	Definition: Request ID. Range: N/A

Table 5-151 TrafficMirrorSession

Parameter	Type	Description
id	String	Definition: ID of a traffic mirror session. After a traffic mirror session is created, a traffic mirror session ID is generated, which uniquely identifies the traffic mirror session. Range: N/A
project_id	String	Definition: ID of the project that a traffic mirror session belongs to. Range: N/A

Parameter	Type	Description
name	String	Definition: Name of a traffic mirror session. Range: The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods.
description	String	Definition: Description of a traffic mirror session. Range: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >).
traffic_mirror_filter_id	String	Definition: ID of the traffic mirror filter that a traffic mirror session is associated with. Range: N/A
traffic_mirror_sources	Array of strings	Definition: IDs of the traffic mirror sources that a traffic mirror session is associated with. Elastic network interfaces can be used as the traffic mirror sources. Range: Each traffic mirror session can have up to 10 mirror sources by default.
traffic_mirror_target_id	String	Definition: ID of the traffic mirror target that a traffic mirror session is associated with. Range: N/A

Parameter	Type	Description
traffic_mirror_target_type	String	Definition: Type of the traffic mirror target that a traffic mirror session is associated with. Range: • eni: The mirror target is an elastic network interface. • elb: The mirror target is a private network load balancer.
virtual_network_id	Integer	Definition: VXLAN network identifier (VNI) of a traffic mirror session, which is used to distinguish different mirror sessions. Range: The value is from 0 to 16777215. The default value is 1.
packet_length	Integer	Definition: Packet length of a traffic mirror session. Range: The value is from 1 to 1460. The default value is 96.
priority	Integer	Definition: Priority of a traffic mirror session. Range: 1 to 32766
enabled	Boolean	Definition: Whether to enable a traffic mirror session. Range: • true: The traffic mirror session is enabled. • false (default value): The traffic mirror session is disabled.

Parameter	Type	Description
type	String	Definition: Type of the traffic mirror source that a traffic mirror session is associated with. Range: • eni: elastic network interface • eip: EIP
created_at	String	Definition: Time when a traffic mirror session was created. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .
updated_at	String	Definition: Time when a traffic mirror session was updated. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .

Table 5-152 PageInfo

Parameter	Type	Description
previous_marker	String	Definition: The first record on the current page. Range: N/A
current_count	Integer	Definition: Total number of resources on the current page. Range: N/A
next_marker	String	Definition: The last record on the current page. The next_marker field does not exist if the page is the last one. Range: N/A

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-eeed-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
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class ListTrafficMirrorSessionsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";
```

```
ICredential auth = new BasicCredentials()
    .withProjectId(projectId)
    .withAk(ak)
    .withSk(sk);

VpcClient client = VpcClient.newBuilder()
    .withCredential(auth)
    .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
    .build();
ListTrafficMirrorSessionsRequest request = new ListTrafficMirrorSessionsRequest();
try {
    ListTrafficMirrorSessionsResponse response = client.listTrafficMirrorSessions(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListTrafficMirrorSessionsRequest()
        response = client.list_traffic_mirror_sessions(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main
```

```
import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListTrafficMirrorSessionsRequest{}
    response, err := client.ListTrafficMirrorSessions(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

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 information about a traffic mirror session, including the name and type.

Calling Method

For details, see [Calling APIs](#).

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	Definition: ID of the project that a traffic mirror session belongs to. For details about how to obtain a project ID, see Obtaining a Project ID . Range: N/A
traffic_mirror_session_id	Yes	String	Definition: ID of a traffic mirror session. Range: N/A

Request Parameters

None

Response Parameters

Status code: 200

Table 5-154 Response body parameters

Parameter	Type	Description
traffic_mirror_session	TrafficMirrorSession object	Definition: Response body for querying details about a traffic mirror session. Range: N/A
request_id	String	Definition: Request ID. Range: N/A

Table 5-155 TrafficMirrorSession

Parameter	Type	Description
id	String	Definition: ID of a traffic mirror session. After a traffic mirror session is created, a traffic mirror session ID is generated, which uniquely identifies the traffic mirror session. Range: N/A
project_id	String	Definition: ID of the project that a traffic mirror session belongs to. Range: N/A
name	String	Definition: Name of a traffic mirror session. Range: The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods.
description	String	Definition: Description of a traffic mirror session. Range: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >).
traffic_mirror_filter_id	String	Definition: ID of the traffic mirror filter that a traffic mirror session is associated with. Range: N/A

Parameter	Type	Description
traffic_mirror_sources	Array of strings	Definition: IDs of the traffic mirror sources that a traffic mirror session is associated with. Elastic network interfaces can be used as the traffic mirror sources. Range: Each traffic mirror session can have up to 10 mirror sources by default.
traffic_mirror_target_id	String	Definition: ID of the traffic mirror target that a traffic mirror session is associated with. Range: N/A
traffic_mirror_target_type	String	Definition: Type of the traffic mirror target that a traffic mirror session is associated with. Range: • eni: The mirror target is an elastic network interface. • elb: The mirror target is a private network load balancer.
virtual_network_id	Integer	Definition: VXLAN network identifier (VNI) of a traffic mirror session, which is used to distinguish different mirror sessions. Range: The value is from 0 to 16777215. The default value is 1.
packet_length	Integer	Definition: Packet length of a traffic mirror session. Range: The value is from 1 to 1460. The default value is 96.
priority	Integer	Definition: Priority of a traffic mirror session. Range: 1 to 32766

Parameter	Type	Description
enabled	Boolean	Definition: Whether to enable a traffic mirror session. Range: true: The traffic mirror session is enabled. false (default value): The traffic mirror session is disabled.
type	String	Definition: Type of the traffic mirror source that a traffic mirror session is associated with. Range: eni: elastic network interface eip: EIP
created_at	String	Definition: Time when a traffic mirror session was created. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .
updated_at	String	Definition: Time when a traffic mirror session was updated. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .

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"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class ShowTrafficMirrorSessionSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();
        ShowTrafficMirrorSessionRequest request = new ShowTrafficMirrorSessionRequest();
        request.withTrafficMirrorSessionId("{traffic_mirror_session_id}");
        try {
            ShowTrafficMirrorSessionResponse response = client.showTrafficMirrorSession(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
        }
    }
}
```

```
        System.out.println(e.getErrorCode());
        System.out.println(e.getErrorMsg());
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowTrafficMirrorSessionRequest()
        request.traffic_mirror_session_id = "{traffic_mirror_session_id}"
        response = client.show_traffic_mirror_session(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
```

```
WithProjectId(projectId).
Build()

client := vpc.NewVpcClient(
    vpc.VpcClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.ShowTrafficMirrorSessionRequest{}
request.TrafficMirrorSessionId = "{traffic_mirror_session_id}"
response, err := client.ShowTrafficMirrorSession(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

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.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v3/{project_id}/vpc/traffic-mirror-sessions

Table 5-156 Path Parameters

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 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.

Parameter	Mandatory	Type	Description
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).
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. - eip: elastic IP.

Response Parameters

Status code: 201

Table 5-159 Response body parameters

Parameter	Type	Description
traffic_mirror_session	TrafficMirrorSession object	Definition: Response body for querying details about a traffic mirror session. Range: N/A
request_id	String	Definition: Request ID. Range: N/A

Table 5-160 TrafficMirrorSession

Parameter	Type	Description
id	String	Definition: ID of a traffic mirror session. After a traffic mirror session is created, a traffic mirror session ID is generated, which uniquely identifies the traffic mirror session. Range: N/A
project_id	String	Definition: ID of the project that a traffic mirror session belongs to. Range: N/A
name	String	Definition: Name of a traffic mirror session. Range: The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods.

Parameter	Type	Description
description	String	Definition: Description of a traffic mirror session. Range: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >).
traffic_mirror_filter_id	String	Definition: ID of the traffic mirror filter that a traffic mirror session is associated with. Range: N/A
traffic_mirror_sources	Array of strings	Definition: IDs of the traffic mirror sources that a traffic mirror session is associated with. Elastic network interfaces can be used as the traffic mirror sources. Range: Each traffic mirror session can have up to 10 mirror sources by default.
traffic_mirror_target_id	String	Definition: ID of the traffic mirror target that a traffic mirror session is associated with. Range: N/A
traffic_mirror_target_type	String	Definition: Type of the traffic mirror target that a traffic mirror session is associated with. Range: • eni: The mirror target is an elastic network interface. • elb: The mirror target is a private network load balancer.

Parameter	Type	Description
virtual_network_id	Integer	Definition: VXLAN network identifier (VNI) of a traffic mirror session, which is used to distinguish different mirror sessions. Range: The value is from 0 to 16777215. The default value is 1.
packet_length	Integer	Definition: Packet length of a traffic mirror session. Range: The value is from 1 to 1460. The default value is 96.
priority	Integer	Definition: Priority of a traffic mirror session. Range: 1 to 32766
enabled	Boolean	Definition: Whether to enable a traffic mirror session. Range: • true: The traffic mirror session is enabled. • false (default value): The traffic mirror session is disabled.
type	String	Definition: Type of the traffic mirror source that a traffic mirror session is associated with. Range: • eni: elastic network interface • eip: EIP
created_at	String	Definition: Time when a traffic mirror session was created. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .

Parameter	Type	Description
updated_at	String	Definition: Time when a traffic mirror session was updated. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .

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"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Create a traffic mirror session named test-session.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

import java.util.List;
import java.util.ArrayList;

public class CreateTrafficMirrorSessionSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();

        CreateTrafficMirrorSessionRequest request = new CreateTrafficMirrorSessionRequest();
        CreateTrafficMirrorSessionRequestBody body = new CreateTrafficMirrorSessionRequestBody();
        List<String> listTrafficMirrorSessionTrafficMirrorSources = new ArrayList<>();
        listTrafficMirrorSessionTrafficMirrorSources.add("6134900d-31a6-4b71-8453-dbca7f26982a");
        CreateTrafficMirrorSessionOption trafficMirrorSessionbody = new CreateTrafficMirrorSessionOption();
        trafficMirrorSessionbody.setName("test-session")
            .withTrafficMirrorFilterId("b765ba87-c0b4-4f1a-9ec3-d5b1d1ddb137")
            .withTrafficMirrorSources(listTrafficMirrorSessionTrafficMirrorSources)
            .withTrafficMirrorTargetId("c9f8acef-d550-4fbe-be7c-e8bfd3501dc1")
            .withTrafficMirrorTargetType("eni")
            .withPriority(11);
        body.withTrafficMirrorSession(trafficMirrorSessionbody);
        request.withBody(body);
        try {
            CreateTrafficMirrorSessionResponse response = client.createTrafficMirrorSession(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrMsg());
        }
    }
}
```

Python

Create a traffic mirror session named test-session.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateTrafficMirrorSessionRequest()
        listTrafficMirrorSourcesTrafficMirrorSession = [
            "6134900d-31a6-4b71-8453-dbca7f26982a"
        ]
        trafficMirrorSessionbody = CreateTrafficMirrorSessionOption(
            name="test-session",
            traffic_mirror_filter_id="b765ba87-c0b4-4f1a-9ec3-d5b1d1ddb137",
            traffic_mirror_sources=listTrafficMirrorSourcesTrafficMirrorSession,
            traffic_mirror_target_id="c9f8acef-d550-4fbe-be7c-e8bfd3501dc1",
            traffic_mirror_target_type="eni",
            priority=11
        )
        request.body = CreateTrafficMirrorSessionRequestBody(
            traffic_mirror_session=trafficMirrorSessionbody
        )
        response = client.create_traffic_mirror_session(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Create a traffic mirror session named test-session.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
```

```
// The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
// In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak := os.Getenv("CLOUD_SDK_AK")
sk := os.Getenv("CLOUD_SDK_SK")
projectId := "{project_id}"

auth := basic.NewCredentialsBuilder().
    WithAk(ak).
    WithSk(sk).
    WithProjectId(projectId).
    Build()

client := vpc.NewVpcClient(
    vpc.VpcClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.CreateTrafficMirrorSessionRequest{}
var listTrafficMirrorSourcesTrafficMirrorSession = []string{
    "6134900d-31a6-4b71-8453-dbca7f26982a",
}
trafficMirrorSessionbody := &model.CreateTrafficMirrorSessionOption{
    Name: "test-session",
    TrafficMirrorFilterId: "b765ba87-c0b4-4f1a-9ec3-d5b1d1ddb137",
    TrafficMirrorSources: listTrafficMirrorSourcesTrafficMirrorSession,
    TrafficMirrorTargetId: "c9f8acef-d550-4fbe-be7c-e8bfd3501dc1",
    TrafficMirrorTargetType: "eni",
    Priority: int32(11),
}
request.Body = &model.CreateTrafficMirrorSessionRequestBody{
    TrafficMirrorSession: trafficMirrorSessionbody,
}
response, err := client.CreateTrafficMirrorSession(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

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.

Calling Method

For details, see [Calling APIs](#).

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. For details about how to obtain a project ID, see Obtaining a 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 (.).

Parameter	Mandatory	Type	Description
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.
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	Definition: Response body for querying details about a traffic mirror session. Range: N/A
request_id	String	Definition: Request ID. Range: N/A

Table 5-165 TrafficMirrorSession

Parameter	Type	Description
id	String	Definition: ID of a traffic mirror session. After a traffic mirror session is created, a traffic mirror session ID is generated, which uniquely identifies the traffic mirror session. Range: N/A
project_id	String	Definition: ID of the project that a traffic mirror session belongs to. Range: N/A
name	String	Definition: Name of a traffic mirror session. Range: The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods.

Parameter	Type	Description
description	String	Definition: Description of a traffic mirror session. Range: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >).
traffic_mirror_filter_id	String	Definition: ID of the traffic mirror filter that a traffic mirror session is associated with. Range: N/A
traffic_mirror_sources	Array of strings	Definition: IDs of the traffic mirror sources that a traffic mirror session is associated with. Elastic network interfaces can be used as the traffic mirror sources. Range: Each traffic mirror session can have up to 10 mirror sources by default.
traffic_mirror_target_id	String	Definition: ID of the traffic mirror target that a traffic mirror session is associated with. Range: N/A
traffic_mirror_target_type	String	Definition: Type of the traffic mirror target that a traffic mirror session is associated with. Range: • eni: The mirror target is an elastic network interface. • elb: The mirror target is a private network load balancer.

Parameter	Type	Description
virtual_network_id	Integer	Definition: VXLAN network identifier (VNI) of a traffic mirror session, which is used to distinguish different mirror sessions. Range: The value is from 0 to 16777215. The default value is 1.
packet_length	Integer	Definition: Packet length of a traffic mirror session. Range: The value is from 1 to 1460. The default value is 96.
priority	Integer	Definition: Priority of a traffic mirror session. Range: 1 to 32766
enabled	Boolean	Definition: Whether to enable a traffic mirror session. Range: • true: The traffic mirror session is enabled. • false (default value): The traffic mirror session is disabled.
type	String	Definition: Type of the traffic mirror source that a traffic mirror session is associated with. Range: • eni: elastic network interface • eip: EIP
created_at	String	Definition: Time when a traffic mirror session was created. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .

Parameter	Type	Description
updated_at	String	Definition: Time when a traffic mirror session was updated. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .

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"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

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.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class UpdateTrafficMirrorSessionSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();
        UpdateTrafficMirrorSessionRequest request = new UpdateTrafficMirrorSessionRequest();
        request.withTrafficMirrorSessionId("{traffic_mirror_session_id}");
        UpdateTrafficMirrorSessionRequestBody body = new UpdateTrafficMirrorSessionRequestBody();
        UpdateTrafficMirrorSessionOption trafficMirrorSessionbody = new UpdateTrafficMirrorSessionOption();
        trafficMirrorSessionbody.withTrafficMirrorTargetId("c9f8acef-d550-4fbe-be7c-e8bfd3501dc1")
            .withTrafficMirrorTargetType("elb");
        body.withTrafficMirrorSession(trafficMirrorSessionbody);
        request.withBody(body);
        try {
            UpdateTrafficMirrorSessionResponse response = client.updateTrafficMirrorSession(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

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.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdateTrafficMirrorSessionRequest()
        request.traffic_mirror_session_id = "{traffic_mirror_session_id}"
        trafficMirrorSessionbody = UpdateTrafficMirrorSessionOption(
            traffic_mirror_target_id="c9f8acef-d550-4fbe-be7c-e8bfd3501dc1",
            traffic_mirror_target_type="elb"
        )
        request.body = UpdateTrafficMirrorSessionRequestBody(
            traffic_mirror_session=trafficMirrorSessionbody
        )
        response = client.update_traffic_mirror_session(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

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.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
```



```
risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
// In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak := os.Getenv("CLOUD_SDK_AK")
sk := os.Getenv("CLOUD_SDK_SK")
projectId := "{project_id}"

auth := basic.NewCredentialsBuilder().
    WithAk(ak).
    WithSk(sk).
    WithProjectId(projectId).
    Build()

client := vpc.NewVpcClient(
    vpc.VpcClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.UpdateTrafficMirrorSessionRequest{}
request.TrafficMirrorSessionId = "{traffic_mirror_session_id}"
trafficMirrorTargetIdTrafficMirrorSession:= "c9f8acef-d550-4fbe-be7c-e8bfd3501dc1"
trafficMirrorTargetTypeTrafficMirrorSession:= "elb"
trafficMirrorSessionbody := &model.UpdateTrafficMirrorSessionOption{
    TrafficMirrorTargetId: &trafficMirrorTargetIdTrafficMirrorSession,
    TrafficMirrorTargetType: &trafficMirrorTargetTypeTrafficMirrorSession,
}
request.Body = &model.UpdateTrafficMirrorSessionRequestBody{
    TrafficMirrorSession: trafficMirrorSessionbody,
}
response, err := client.UpdateTrafficMirrorSession(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

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.

Calling Method

For details, see [Calling APIs](#).

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. For details about how to obtain a project ID, see Obtaining a Project ID .
traffic_mirror_session_id	Yes	String	Traffic mirror session ID.

Request Parameters

None

Response Parameters

Status code: 204

No Content

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

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
```

```
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class DeleteTrafficMirrorSessionSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();
        DeleteTrafficMirrorSessionRequest request = new DeleteTrafficMirrorSessionRequest();
        request.withTrafficMirrorSessionId("{traffic_mirror_session_id}");
        try {
            DeleteTrafficMirrorSessionResponse response = client.deleteTrafficMirrorSession(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
```

```
.with_credentials(credentials) \
.with_region(VpcRegion.value_of("<YOUR REGION>")) \
.build()

try:
    request = DeleteTrafficMirrorSessionRequest()
    request.traffic_mirror_session_id = "{traffic_mirror_session_id}"
    response = client.delete_traffic_mirror_session(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteTrafficMirrorSessionRequest{
        request.TrafficMirrorSessionId = "{traffic_mirror_session_id}"
    }
    response, err := client.DeleteTrafficMirrorSession(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

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.

Calling Method

For details, see [Calling APIs](#).

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. For details about how to obtain a project ID, see Obtaining a 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	Definition: Response body for querying details about a traffic mirror session. Range: N/A
request_id	String	Definition: Request ID. Range: N/A

Table 5-171 TrafficMirrorSession

Parameter	Type	Description
id	String	Definition: ID of a traffic mirror session. After a traffic mirror session is created, a traffic mirror session ID is generated, which uniquely identifies the traffic mirror session. Range: N/A
project_id	String	Definition: ID of the project that a traffic mirror session belongs to. Range: N/A

Parameter	Type	Description
name	String	Definition: Name of a traffic mirror session. Range: The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods.
description	String	Definition: Description of a traffic mirror session. Range: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >).
traffic_mirror_filter_id	String	Definition: ID of the traffic mirror filter that a traffic mirror session is associated with. Range: N/A
traffic_mirror_sources	Array of strings	Definition: IDs of the traffic mirror sources that a traffic mirror session is associated with. Elastic network interfaces can be used as the traffic mirror sources. Range: Each traffic mirror session can have up to 10 mirror sources by default.
traffic_mirror_target_id	String	Definition: ID of the traffic mirror target that a traffic mirror session is associated with. Range: N/A

Parameter	Type	Description
traffic_mirror_target_type	String	Definition: Type of the traffic mirror target that a traffic mirror session is associated with. Range: • eni: The mirror target is an elastic network interface. • elb: The mirror target is a private network load balancer.
virtual_network_id	Integer	Definition: VXLAN network identifier (VNI) of a traffic mirror session, which is used to distinguish different mirror sessions. Range: The value is from 0 to 16777215. The default value is 1.
packet_length	Integer	Definition: Packet length of a traffic mirror session. Range: The value is from 1 to 1460. The default value is 96.
priority	Integer	Definition: Priority of a traffic mirror session. Range: 1 to 32766
enabled	Boolean	Definition: Whether to enable a traffic mirror session. Range: • true: The traffic mirror session is enabled. • false (default value): The traffic mirror session is disabled.

Parameter	Type	Description
type	String	Definition: Type of the traffic mirror source that a traffic mirror session is associated with. Range: • eni: elastic network interface • eip: EIP
created_at	String	Definition: Time when a traffic mirror session was created. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .
updated_at	String	Definition: Time when a traffic mirror session was updated. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .

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"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Disassociate the mirror source with ID of 6134900d-31a6-4b71-8453-dbca7f26982a from the mirror session with ID of e15a6e40-2580-4949-bf2a-55ee7cd49392.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

import java.util.List;
import java.util.ArrayList;

public class RemoveSourcesFromTrafficMirrorSessionSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();

        RemoveSourcesFromTrafficMirrorSessionRequest request = new
        RemoveSourcesFromTrafficMirrorSessionRequest();
        request.withTrafficMirrorSessionId("{traffic_mirror_session_id}");
        RemoveSourcesFromTrafficMirrorSessionRequestBody body = new
        RemoveSourcesFromTrafficMirrorSessionRequestBody();
        List<String> listTrafficMirrorSessionTrafficMirrorSources = new ArrayList<>();
        listTrafficMirrorSessionTrafficMirrorSources.add("6134900d-31a6-4b71-8453-dbca7f26982a");
        TrafficMirrorSourcesOption trafficMirrorSessionbody = new TrafficMirrorSourcesOption();
        trafficMirrorSessionbody.withTrafficMirrorSources(listTrafficMirrorSessionTrafficMirrorSources);
        body.withTrafficMirrorSession(trafficMirrorSessionbody);
    }
}
```

```
request.withBody(body);
try {
    RemoveSourcesFromTrafficMirrorSessionResponse response =
client.removeSourcesFromTrafficMirrorSession(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

Disassociate the mirror source with ID of 6134900d-31a6-4b71-8453-dbca7f26982a from the mirror session with ID of e15a6e40-2580-4949-bf2a-55ee7cd49392.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = RemoveSourcesFromTrafficMirrorSessionRequest()
        request.traffic_mirror_session_id = "{traffic_mirror_session_id}"
        listTrafficMirrorSourcesTrafficMirrorSession = [
            "6134900d-31a6-4b71-8453-dbca7f26982a"
        ]
        trafficMirrorSessionbody = TrafficMirrorSourcesOption(
            traffic_mirror_sources=listTrafficMirrorSourcesTrafficMirrorSession
        )
        request.body = RemoveSourcesFromTrafficMirrorSessionRequestBody(
            traffic_mirror_session=trafficMirrorSessionbody
        )
        response = client.remove_sources_from_traffic_mirror_session(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
```

```
print(e.error_code)
print(e.error_msg)
```

Go

Disassociate the mirror source with ID of 6134900d-31a6-4b71-8453-dbca7f26982a from the mirror session with ID of e15a6e40-2580-4949-bf2a-55ee7cd49392.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.RemoveSourcesFromTrafficMirrorSessionRequest{}
    request.TrafficMirrorSessionId = "{traffic_mirror_session_id}"
    var listTrafficMirrorSourcesTrafficMirrorSession = []string{
        "6134900d-31a6-4b71-8453-dbca7f26982a",
    }
    trafficMirrorSessionbody := &model.TrafficMirrorSourcesOption{
        TrafficMirrorSources: listTrafficMirrorSourcesTrafficMirrorSession,
    }
    request.Body = &model.RemoveSourcesFromTrafficMirrorSessionRequestBody{
        TrafficMirrorSession: trafficMirrorSessionbody,
    }
    response, err := client.RemoveSourcesFromTrafficMirrorSession(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

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.

Calling Method

For details, see [Calling APIs](#).

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. For details about how to obtain a project ID, see Obtaining a 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	Definition: Response body for querying details about a traffic mirror session. Range: N/A
request_id	String	Definition: Request ID. Range: N/A

Table 5-176 TrafficMirrorSession

Parameter	Type	Description
id	String	Definition: ID of a traffic mirror session. After a traffic mirror session is created, a traffic mirror session ID is generated, which uniquely identifies the traffic mirror session. Range: N/A
project_id	String	Definition: ID of the project that a traffic mirror session belongs to. Range: N/A

Parameter	Type	Description
name	String	Definition: Name of a traffic mirror session. Range: The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods.
description	String	Definition: Description of a traffic mirror session. Range: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >).
traffic_mirror_filter_id	String	Definition: ID of the traffic mirror filter that a traffic mirror session is associated with. Range: N/A
traffic_mirror_sources	Array of strings	Definition: IDs of the traffic mirror sources that a traffic mirror session is associated with. Elastic network interfaces can be used as the traffic mirror sources. Range: Each traffic mirror session can have up to 10 mirror sources by default.
traffic_mirror_target_id	String	Definition: ID of the traffic mirror target that a traffic mirror session is associated with. Range: N/A

Parameter	Type	Description
traffic_mirror_target_type	String	Definition: Type of the traffic mirror target that a traffic mirror session is associated with. Range: • eni: The mirror target is an elastic network interface. • elb: The mirror target is a private network load balancer.
virtual_network_id	Integer	Definition: VXLAN network identifier (VNI) of a traffic mirror session, which is used to distinguish different mirror sessions. Range: The value is from 0 to 16777215. The default value is 1.
packet_length	Integer	Definition: Packet length of a traffic mirror session. Range: The value is from 1 to 1460. The default value is 96.
priority	Integer	Definition: Priority of a traffic mirror session. Range: 1 to 32766
enabled	Boolean	Definition: Whether to enable a traffic mirror session. Range: • true: The traffic mirror session is enabled. • false (default value): The traffic mirror session is disabled.

Parameter	Type	Description
type	String	Definition: Type of the traffic mirror source that a traffic mirror session is associated with. Range: • eni: elastic network interface • eip: EIP
created_at	String	Definition: Time when a traffic mirror session was created. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .
updated_at	String	Definition: Time when a traffic mirror session was updated. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .

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

Normal response to the PUT operation. For more status codes, see [Status Codes](#).

```
{
  "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"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Associate the mirror source 6134900d-31a6-4b71-8453-dbca7f26982e with the mirror session e15a6e40-2580-4949-bf2a-55ee7cd49392.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

import java.util.List;
import java.util.ArrayList;

public class AddSourcesToTrafficMirrorSessionSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();

        AddSourcesToTrafficMirrorSessionRequest request = new AddSourcesToTrafficMirrorSessionRequest();
        request.withTrafficMirrorSessionId("{traffic_mirror_session_id}");
        AddSourcesToTrafficMirrorSessionRequestBody body = new
        AddSourcesToTrafficMirrorSessionRequestBody();
        List<String> listTrafficMirrorSessionTrafficMirrorSources = new ArrayList<>();
        listTrafficMirrorSessionTrafficMirrorSources.add("6134900d-31a6-4b71-8453-dbca7f26982e");
        TrafficMirrorSourcesOption trafficMirrorSessionbody = new TrafficMirrorSourcesOption();
        trafficMirrorSessionbody.withTrafficMirrorSources(listTrafficMirrorSessionTrafficMirrorSources);
        body.withTrafficMirrorSession(trafficMirrorSessionbody);
        request.withBody(body);
        try {
            AddSourcesToTrafficMirrorSessionResponse response =
```

```
client.addSourcesToTrafficMirrorSession(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

Associate the mirror source 6134900d-31a6-4b71-8453-dbca7f26982e with the mirror session e15a6e40-2580-4949-bf2a-55ee7cd49392.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = AddSourcesToTrafficMirrorSessionRequest()
        request.traffic_mirror_session_id = "{traffic_mirror_session_id}"
        listTrafficMirrorSourcesTrafficMirrorSession = [
            "6134900d-31a6-4b71-8453-dbca7f26982e"
        ]
        trafficMirrorSessionbody = TrafficMirrorSourcesOption(
            traffic_mirror_sources=listTrafficMirrorSourcesTrafficMirrorSession
        )
        request.body = AddSourcesToTrafficMirrorSessionRequestBody(
            traffic_mirror_session=trafficMirrorSessionbody
        )
        response = client.add_sources_to_traffic_mirror_session(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Associate the mirror source 6134900d-31a6-4b71-8453-dbca7f26982e with the mirror session e15a6e40-2580-4949-bf2a-55ee7cd49392.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.AddSourcesToTrafficMirrorSessionRequest{}
    request.TrafficMirrorSessionId = "{traffic_mirror_session_id}"
    var listTrafficMirrorSourcesTrafficMirrorSession = []string{
        "6134900d-31a6-4b71-8453-dbca7f26982e",
    }
    trafficMirrorSessionbody := &model.TrafficMirrorSourcesOption{
        TrafficMirrorSources: listTrafficMirrorSourcesTrafficMirrorSession,
    }
    request.Body = &model.AddSourcesToTrafficMirrorSessionRequestBody{
        TrafficMirrorSession: trafficMirrorSessionbody,
    }
    response, err := client.AddSourcesToTrafficMirrorSession(request)
    if err == nil {
        fmt.Printf("%v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Normal response to the PUT operation. For more status codes, see Status Codes .

Error Codes

See [Error Codes](#).

5.7 Traffic Mirror Filters

5.7.1 Creating a Traffic Mirror Filter

Function

Traffic mirror filters filter specified traffic for mirroring. This API is used to create a traffic mirror filter. A mirror filter is a set of inbound rules and outbound rules to determine the traffic that is mirrored. You can specify priority, action, and other match conditions for each rule.

- Inbound rules match the traffic received by a mirror source.
- Outbound rules match the traffic sent by a mirror source.

A mirror filter takes effect only after it is associated with mirror sessions.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v3/{project_id}/vpc/traffic-mirror-filters

Table 5-177 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: ID of the project that a traffic mirror filter belongs to. For details about how to obtain a project ID, see Obtaining a Project ID . Range: N/A

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	Definition: Response body for querying details about a traffic mirror filter. Range: N/A
request_id	String	Definition: Request ID. Range: N/A

Table 5-181 TrafficMirrorFilter

Parameter	Type	Description
id	String	Definition: ID of a traffic mirror filter. After a traffic mirror filter is created, a traffic mirror filter ID is generated, which uniquely identifies the traffic mirror filter. Range: N/A
project_id	String	Definition: ID of the project that a traffic mirror filter belongs to. Range: N/A
description	String	Definition: Description of a traffic mirror filter. Range: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >).
name	String	Definition: Name of a traffic mirror filter. Range: The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods.
ingress_rules	Array of TrafficMirrorFilterRule objects	Definition: Inbound mirror filter rules in a traffic mirror filter. Range: N/A
egress_rules	Array of TrafficMirrorFilterRule objects	Definition: Outbound mirror filter rules in a traffic mirror filter. Range: N/A

Parameter	Type	Description
created_at	String	Definition: Time when a traffic mirror filter was created. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .
updated_at	String	Definition: Time when a traffic mirror filter was updated. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .
type	String	Definition: Mirror source type of a traffic mirror filter. Range: • eni: elastic network interface

Table 5-182 TrafficMirrorFilterRule

Parameter	Type	Description
id	String	Definition: ID of a traffic mirror filter rule. Range: N/A
project_id	String	Definition: ID of the project that a traffic mirror filter rule belongs to. Range: N/A
description	String	Definition: Description of a traffic mirror filter rule. Range: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >).

Parameter	Type	Description
traffic_mirror_filter_id	String	Definition: ID of the traffic mirror filter that a traffic mirror filter rule belongs to. Range: N/A
direction	String	Definition: Traffic direction of a traffic mirror filter rule. Range: • ingress: inbound traffic • egress: outbound traffic
source_cidr_block	String	Definition: Source of a traffic mirror filter rule. Range: • Single IP address: IP address/subnet mask. For example, 192.168.10.10/32 for a single IPv4 address or 2002:50::44/128 for a single IPv6 address. • CIDR block: IP address/subnet mask. For example, 192.168.52.0/24 for an IPv4 CIDR block or 2407:c080:802:469::/64 for an IPv6 CIDR block. • All IP addresses: 0.0.0.0/0 indicates all IPv4 addresses, and ::/0 indicates all IPv6 addresses.

Parameter	Type	Description
destination_cidr_block	String	Definition: Destination of a traffic mirror filter rule. Range: - Single IP address: IP address/subnet mask. For example, 192.168.10.10/32 for a single IPv4 address or 2002:50::44/128 for a single IPv6 address. - CIDR block: IP address/subnet mask. For example, 192.168.52.0/24 for an IPv4 CIDR block or 2407:c080:802:469::/64 for an IPv6 CIDR block. - All IP addresses: 0.0.0.0/0 indicates all IPv4 addresses, and ::/0 indicates all IPv6 addresses.
source_port_range	String	Definition: Source port range of a traffic mirror filter rule. Range: - Port range: 1 to 65535 - Use a hyphen (-) to connect the start port and the end port, for example, 22-23. The end port cannot be smaller than the start port.
destination_port_range	String	Definition: Destination port range of a traffic mirror filter rule. Range: - Port range: 1 to 65535 - Use a hyphen (-) to connect the start port and the end port, for example, 22-23. The end port cannot be smaller than the start port.
ethertype	String	Definition: IP address version. Range: IPv4 or IPv6

Parameter	Type	Description
protocol	String	Definition: Network protocol type. Range: • TCP: If you select TCP, you can customize the source and destination port ranges. • UDP: If you select UDP, you can customize the source and destination port ranges. • ICMP: If you set IP address version to IPv4 and select ICMP, all ports are specified for source and destination port ranges by default. • ICMPV6: If you set IP address version to IPv6 and select ICMPv6, all ports are specified for source and destination port ranges by default. • ALL: If you select ALL, all network protocols are supported and all ports are specified for source and destination port ranges by default.
action	String	Definition: Action of a traffic mirror filter rule. Range: • accept • reject
priority	Integer	Definition: Priority of a traffic mirror filter rule. Range: The value is from 1 to 65535. A smaller value indicates a higher priority.
created_at	String	Definition: Time when a traffic mirror filter rule was created. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .

Parameter	Type	Description
updated_at	String	Definition: Time when a traffic mirror filter rule was updated. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .

Example Requests

Create a traffic mirror filter named **test1** with description set to **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" : [ ],
    "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"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Create a traffic mirror filter named **test1** with description set to **description**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
```

```
import com.huaweicloud.sdk.vpc.v3.model.*;

public class CreateTrafficMirrorFilterSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();
        CreateTrafficMirrorFilterRequest request = new CreateTrafficMirrorFilterRequest();
        CreateTrafficMirrorFilterRequestBody body = new CreateTrafficMirrorFilterRequestBody();
        CreateTrafficMirrorFilterOption trafficMirrorFilterbody = new CreateTrafficMirrorFilterOption();
        trafficMirrorFilterbody.withDescription("description")
            .withName("test1");
        body.withTrafficMirrorFilter(trafficMirrorFilterbody);
        request.withBody(body);
        try {
            CreateTrafficMirrorFilterResponse response = client.createTrafficMirrorFilter(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Create a traffic mirror filter named **test1** with description set to **description**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"
```

```
credentials = BasicCredentials(ak, sk, projectId)

client = VpcClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(VpcRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = CreateTrafficMirrorFilterRequest()
    trafficMirrorFilterbody = CreateTrafficMirrorFilterOption(
        description="description",
        name="test1"
    )
    request.body = CreateTrafficMirrorFilterRequestBody(
        traffic_mirror_filter=trafficMirrorFilterbody
    )
    response = client.create_traffic_mirror_filter(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

Create a traffic mirror filter named **test1** with description set to **description**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateTrafficMirrorFilterRequest{
        descriptionTrafficMirrorFilter:= "description"
    }
    trafficMirrorFilterbody := &model.CreateTrafficMirrorFilterOption{
        Description: &descriptionTrafficMirrorFilter,
        Name: "test1",
    }
    request.Body = &model.CreateTrafficMirrorFilterRequestBody{
        TrafficMirrorFilter: trafficMirrorFilterbody,
    }
```

```
}
response, err := client.CreateTrafficMirrorFilter(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

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 information about all traffic mirror filters, including the name and type.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v3/{project_id}/vpc/traffic-mirror-filters

Table 5-183 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: ID of the project that a traffic mirror filter belongs to. For details about how to obtain a project ID, see Obtaining a Project ID . Range: N/A

Table 5-184 Query Parameters

Parameter	Mandatory	Type	Description
id	No	Array of strings	Definition: ID of a traffic mirror filter. You can use this field to accurately filter traffic mirror filters. Multiple IDs can be specified for filtering. Range: N/A
name	No	Array of strings	Definition: Name of a traffic mirror filter. You can use this field to filter traffic mirror filters. Multiple names can be specified for filtering. Range: N/A
description	No	Array of strings	Definition: Description of a traffic mirror filter. You can use this field to filter traffic mirror filters. Multiple descriptions can be specified for filtering. Range: N/A

Request Parameters

None

Response Parameters

Status code: 200

Table 5-185 Response body parameters

Parameter	Type	Description
traffic_mirror_filters	Array of TrafficMirrorFilter objects	Definition: Response body for querying traffic mirror filters. Range: N/A
page_info	PageInfo object	Definition: Pagination information. Range: N/A
request_id	String	Definition: Request ID. Range: N/A

Table 5-186 TrafficMirrorFilter

Parameter	Type	Description
id	String	Definition: ID of a traffic mirror filter. After a traffic mirror filter is created, a traffic mirror filter ID is generated, which uniquely identifies the traffic mirror filter. Range: N/A
project_id	String	Definition: ID of the project that a traffic mirror filter belongs to. Range: N/A

Parameter	Type	Description
description	String	Definition: Description of a traffic mirror filter. Range: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >).
name	String	Definition: Name of a traffic mirror filter. Range: The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods.
ingress_rules	Array of TrafficMirrorFilterRule objects	Definition: Inbound mirror filter rules in a traffic mirror filter. Range: N/A
egress_rules	Array of TrafficMirrorFilterRule objects	Definition: Outbound mirror filter rules in a traffic mirror filter. Range: N/A
created_at	String	Definition: Time when a traffic mirror filter was created. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .
updated_at	String	Definition: Time when a traffic mirror filter was updated. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .
type	String	Definition: Mirror source type of a traffic mirror filter. Range: eni: elastic network interface

Table 5-187 TrafficMirrorFilterRule

Parameter	Type	Description
id	String	Definition: ID of a traffic mirror filter rule. Range: N/A
project_id	String	Definition: ID of the project that a traffic mirror filter rule belongs to. Range: N/A
description	String	Definition: Description of a traffic mirror filter rule. Range: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >).
traffic_mirror_filter_id	String	Definition: ID of the traffic mirror filter that a traffic mirror filter rule belongs to. Range: N/A
direction	String	Definition: Traffic direction of a traffic mirror filter rule. Range: • ingress: inbound traffic • egress: outbound traffic

Parameter	Type	Description
source_cidr_block	String	Definition: Source of a traffic mirror filter rule. Range: - Single IP address: IP address/subnet mask. For example, 192.168.10.10/32 for a single IPv4 address or 2002:50::44/128 for a single IPv6 address. - CIDR block: IP address/subnet mask. For example, 192.168.52.0/24 for an IPv4 CIDR block or 2407:c080:802:469::/64 for an IPv6 CIDR block. - All IP addresses: 0.0.0.0/0 indicates all IPv4 addresses, and ::/0 indicates all IPv6 addresses.
destination_cidr_block	String	Definition: Destination of a traffic mirror filter rule. Range: - Single IP address: IP address/subnet mask. For example, 192.168.10.10/32 for a single IPv4 address or 2002:50::44/128 for a single IPv6 address. - CIDR block: IP address/subnet mask. For example, 192.168.52.0/24 for an IPv4 CIDR block or 2407:c080:802:469::/64 for an IPv6 CIDR block. - All IP addresses: 0.0.0.0/0 indicates all IPv4 addresses, and ::/0 indicates all IPv6 addresses.
source_port_range	String	Definition: Source port range of a traffic mirror filter rule. Range: - Port range: 1 to 65535 - Use a hyphen (-) to connect the start port and the end port, for example, 22-23. The end port cannot be smaller than the start port.

Parameter	Type	Description
destination_port_range	String	Definition: Destination port range of a traffic mirror filter rule. Range: - Port range: 1 to 65535 - Use a hyphen (-) to connect the start port and the end port, for example, 22-23. The end port cannot be smaller than the start port.
ethertype	String	Definition: IP address version. Range: IPv4 or IPv6
protocol	String	Definition: Network protocol type. Range: TCP: If you select TCP, you can customize the source and destination port ranges. UDP: If you select UDP, you can customize the source and destination port ranges. ICMP: If you set IP address version to IPv4 and select ICMP, all ports are specified for source and destination port ranges by default. ICMPV6: If you set IP address version to IPv6 and select ICMPv6, all ports are specified for source and destination port ranges by default. ALL: If you select ALL, all network protocols are supported and all ports are specified for source and destination port ranges by default.
action	String	Definition: Action of a traffic mirror filter rule. Range: accept reject

Parameter	Type	Description
priority	Integer	Definition: Priority of a traffic mirror filter rule. Range: The value is from 1 to 65535. A smaller value indicates a higher priority.
created_at	String	Definition: Time when a traffic mirror filter rule was created. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .
updated_at	String	Definition: Time when a traffic mirror filter rule was updated. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .

Table 5-188 PageInfo

Parameter	Type	Description
previous_marker	String	Definition: The first record on the current page. Range: N/A
current_count	Integer	Definition: Total number of resources on the current page. Range: N/A
next_marker	String	Definition: The last record on the current page. The next_marker field does not exist if the page is the last one. Range: N/A

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" : [ ],
    "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
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class ListTrafficMirrorFiltersSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
```

```
        .withCredential(auth)
        .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
        .build();
ListTrafficMirrorFiltersRequest request = new ListTrafficMirrorFiltersRequest();
try {
    ListTrafficMirrorFiltersResponse response = client.listTrafficMirrorFilters(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListTrafficMirrorFiltersRequest()
        response = client.list_traffic_mirror_filters(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)
```



```
func main() {  
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security  
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment  
    // variables and decrypted during use to ensure security.  
    // In this example, AK and SK are stored in environment variables for authentication. Before running this  
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak := os.Getenv("CLOUD_SDK_AK")  
    sk := os.Getenv("CLOUD_SDK_SK")  
    projectId := "{project_id}"  
  
    auth := basic.NewCredentialsBuilder().  
        WithAk(ak).  
        WithSk(sk).  
        WithProjectId(projectId).  
        Build()  
  
    client := vpc.NewVpcClient(  
        vpc.VpcClientBuilder().  
            WithRegion(region.ValueOf("<YOUR REGION>")).  
            WithCredential(auth).  
            Build()  
    )  
  
    request := &model.ListTrafficMirrorFiltersRequest{}  
    response, err := client.ListTrafficMirrorFilters(request)  
    if err == nil {  
        fmt.Printf("%+v\n", response)  
    } else {  
        fmt.Println(err)  
    }  
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

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 information about a traffic mirror filter, including the name and type.

Calling Method

For details, see [Calling APIs](#).

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	Definition: ID of the project that a traffic mirror filter belongs to. For details about how to obtain a project ID, see Obtaining a Project ID . Range: N/A
traffic_mirror_filter_id	Yes	String	Definition: ID of a traffic mirror filter. Range: N/A

Request Parameters

None

Response Parameters

Status code: 200

Table 5-190 Response body parameters

Parameter	Type	Description
traffic_mirror_filter	TrafficMirrorFilter object	Definition: Response body for querying details about a traffic mirror filter. Range: N/A
request_id	String	Definition: Request ID. Range: N/A

Table 5-191 TrafficMirrorFilter

Parameter	Type	Description
id	String	Definition: ID of a traffic mirror filter. After a traffic mirror filter is created, a traffic mirror filter ID is generated, which uniquely identifies the traffic mirror filter. Range: N/A
project_id	String	Definition: ID of the project that a traffic mirror filter belongs to. Range: N/A
description	String	Definition: Description of a traffic mirror filter. Range: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >).
name	String	Definition: Name of a traffic mirror filter. Range: The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods.
ingress_rules	Array of TrafficMirrorFilterRule objects	Definition: Inbound mirror filter rules in a traffic mirror filter. Range: N/A
egress_rules	Array of TrafficMirrorFilterRule objects	Definition: Outbound mirror filter rules in a traffic mirror filter. Range: N/A

Parameter	Type	Description
created_at	String	Definition: Time when a traffic mirror filter was created. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .
updated_at	String	Definition: Time when a traffic mirror filter was updated. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .
type	String	Definition: Mirror source type of a traffic mirror filter. Range: • eni: elastic network interface

Table 5-192 TrafficMirrorFilterRule

Parameter	Type	Description
id	String	Definition: ID of a traffic mirror filter rule. Range: N/A
project_id	String	Definition: ID of the project that a traffic mirror filter rule belongs to. Range: N/A
description	String	Definition: Description of a traffic mirror filter rule. Range: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >).

Parameter	Type	Description
traffic_mirror_filter_id	String	Definition: ID of the traffic mirror filter that a traffic mirror filter rule belongs to. Range: N/A
direction	String	Definition: Traffic direction of a traffic mirror filter rule. Range: • ingress: inbound traffic • egress: outbound traffic
source_cidr_block	String	Definition: Source of a traffic mirror filter rule. Range: • Single IP address: IP address/subnet mask. For example, 192.168.10.10/32 for a single IPv4 address or 2002:50::44/128 for a single IPv6 address. • CIDR block: IP address/subnet mask. For example, 192.168.52.0/24 for an IPv4 CIDR block or 2407:c080:802:469::/64 for an IPv6 CIDR block. • All IP addresses: 0.0.0.0/0 indicates all IPv4 addresses, and ::/0 indicates all IPv6 addresses.

Parameter	Type	Description
destination_cidr_block	String	Definition: Destination of a traffic mirror filter rule. Range: • Single IP address: IP address/subnet mask. For example, 192.168.10.10/32 for a single IPv4 address or 2002:50::44/128 for a single IPv6 address. • CIDR block: IP address/subnet mask. For example, 192.168.52.0/24 for an IPv4 CIDR block or 2407:c080:802:469::/64 for an IPv6 CIDR block. • All IP addresses: 0.0.0.0/0 indicates all IPv4 addresses, and ::/0 indicates all IPv6 addresses.
source_port_range	String	Definition: Source port range of a traffic mirror filter rule. Range: • Port range: 1 to 65535 • Use a hyphen (-) to connect the start port and the end port, for example, 22-23. The end port cannot be smaller than the start port.
destination_port_range	String	Definition: Destination port range of a traffic mirror filter rule. Range: • Port range: 1 to 65535 • Use a hyphen (-) to connect the start port and the end port, for example, 22-23. The end port cannot be smaller than the start port.
ethertype	String	Definition: IP address version. Range: IPv4 or IPv6

Parameter	Type	Description
protocol	String	Definition: Network protocol type. Range: • TCP: If you select TCP, you can customize the source and destination port ranges. • UDP: If you select UDP, you can customize the source and destination port ranges. • ICMP: If you set IP address version to IPv4 and select ICMP, all ports are specified for source and destination port ranges by default. • ICMPV6: If you set IP address version to IPv6 and select ICMPv6, all ports are specified for source and destination port ranges by default. • ALL: If you select ALL, all network protocols are supported and all ports are specified for source and destination port ranges by default.
action	String	Definition: Action of a traffic mirror filter rule. Range: • accept • reject
priority	Integer	Definition: Priority of a traffic mirror filter rule. Range: The value is from 1 to 65535. A smaller value indicates a higher priority.
created_at	String	Definition: Time when a traffic mirror filter rule was created. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .

Parameter	Type	Description
updated_at	String	Definition: Time when a traffic mirror filter rule was updated. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .

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" : [ ],
    "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"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class ShowTrafficMirrorFilterSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
    }
}
```



```
// In this example, AK and SK are stored in environment variables for authentication. Before running
this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
String ak = System.getenv("CLOUD_SDK_AK");
String sk = System.getenv("CLOUD_SDK_SK");
String projectId = "{project_id}";

ICredential auth = new BasicCredentials()
    .withProjectId(projectId)
    .withAk(ak)
    .withSk(sk);

VpcClient client = VpcClient.newBuilder()
    .withCredential(auth)
    .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
    .build();
ShowTrafficMirrorFilterRequest request = new ShowTrafficMirrorFilterRequest();
request.withTrafficMirrorFilterId("{traffic_mirror_filter_id}");
try {
    ShowTrafficMirrorFilterResponse response = client.showTrafficMirrorFilter(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowTrafficMirrorFilterRequest()
        request.traffic_mirror_filter_id = "{traffic_mirror_filter_id}"
        response = client.show_traffic_mirror_filter(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
```

```
print(e.error_code)
print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowTrafficMirrorFilterRequest{}
    request.TrafficMirrorFilterId = "{traffic_mirror_filter_id}"
    response, err := client.ShowTrafficMirrorFilter(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

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.

Calling Method

For details, see [Calling APIs](#).

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. For details about how to obtain a project ID, see Obtaining a 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 >).

Parameter	Mandatory	Type	Description
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	Definition: Response body for querying details about a traffic mirror filter. Range: N/A
request_id	String	Definition: Request ID. Range: N/A

Table 5-197 TrafficMirrorFilter

Parameter	Type	Description
id	String	Definition: ID of a traffic mirror filter. After a traffic mirror filter is created, a traffic mirror filter ID is generated, which uniquely identifies the traffic mirror filter. Range: N/A
project_id	String	Definition: ID of the project that a traffic mirror filter belongs to. Range: N/A

Parameter	Type	Description
description	String	Definition: Description of a traffic mirror filter. Range: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >).
name	String	Definition: Name of a traffic mirror filter. Range: The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods.
ingress_rules	Array of TrafficMirrorFilterRule objects	Definition: Inbound mirror filter rules in a traffic mirror filter. Range: N/A
egress_rules	Array of TrafficMirrorFilterRule objects	Definition: Outbound mirror filter rules in a traffic mirror filter. Range: N/A
created_at	String	Definition: Time when a traffic mirror filter was created. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .
updated_at	String	Definition: Time when a traffic mirror filter was updated. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .
type	String	Definition: Mirror source type of a traffic mirror filter. Range: eni: elastic network interface

Table 5-198 TrafficMirrorFilterRule

Parameter	Type	Description
id	String	Definition: ID of a traffic mirror filter rule. Range: N/A
project_id	String	Definition: ID of the project that a traffic mirror filter rule belongs to. Range: N/A
description	String	Definition: Description of a traffic mirror filter rule. Range: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >).
traffic_mirror_filter_id	String	Definition: ID of the traffic mirror filter that a traffic mirror filter rule belongs to. Range: N/A
direction	String	Definition: Traffic direction of a traffic mirror filter rule. Range: • ingress: inbound traffic • egress: outbound traffic

Parameter	Type	Description
source_cidr_block	String	Definition: Source of a traffic mirror filter rule. Range: - Single IP address: IP address/subnet mask. For example, 192.168.10.10/32 for a single IPv4 address or 2002:50::44/128 for a single IPv6 address. - CIDR block: IP address/subnet mask. For example, 192.168.52.0/24 for an IPv4 CIDR block or 2407:c080:802:469::/64 for an IPv6 CIDR block. - All IP addresses: 0.0.0.0/0 indicates all IPv4 addresses, and ::/0 indicates all IPv6 addresses.
destination_cidr_block	String	Definition: Destination of a traffic mirror filter rule. Range: - Single IP address: IP address/subnet mask. For example, 192.168.10.10/32 for a single IPv4 address or 2002:50::44/128 for a single IPv6 address. - CIDR block: IP address/subnet mask. For example, 192.168.52.0/24 for an IPv4 CIDR block or 2407:c080:802:469::/64 for an IPv6 CIDR block. - All IP addresses: 0.0.0.0/0 indicates all IPv4 addresses, and ::/0 indicates all IPv6 addresses.
source_port_range	String	Definition: Source port range of a traffic mirror filter rule. Range: - Port range: 1 to 65535 - Use a hyphen (-) to connect the start port and the end port, for example, 22-23. The end port cannot be smaller than the start port.

Parameter	Type	Description
destination_port_range	String	Definition: Destination port range of a traffic mirror filter rule. Range: - Port range: 1 to 65535 - Use a hyphen (-) to connect the start port and the end port, for example, 22-23. The end port cannot be smaller than the start port.
ethertype	String	Definition: IP address version. Range: IPv4 or IPv6
protocol	String	Definition: Network protocol type. Range: TCP: If you select TCP, you can customize the source and destination port ranges. UDP: If you select UDP, you can customize the source and destination port ranges. ICMP: If you set IP address version to IPv4 and select ICMP, all ports are specified for source and destination port ranges by default. ICMPV6: If you set IP address version to IPv6 and select ICMPv6, all ports are specified for source and destination port ranges by default. ALL: If you select ALL, all network protocols are supported and all ports are specified for source and destination port ranges by default.
action	String	Definition: Action of a traffic mirror filter rule. Range: accept reject

Parameter	Type	Description
priority	Integer	Definition: Priority of a traffic mirror filter rule. Range: The value is from 1 to 65535. A smaller value indicates a higher priority.
created_at	String	Definition: Time when a traffic mirror filter rule was created. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .
updated_at	String	Definition: Time when a traffic mirror filter rule was updated. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .

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" : [ ],
    "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"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Change the name of the traffic mirror filter whose ID is 59d2b2e7-0d35-41f7-a12e-f7699366cd21 to test1.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class UpdateTrafficMirrorFilterSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();

        UpdateTrafficMirrorFilterRequest request = new UpdateTrafficMirrorFilterRequest();
        request.withTrafficMirrorFilterId("{traffic_mirror_filter_id}");
        UpdateTrafficMirrorFilterRequestBody body = new UpdateTrafficMirrorFilterRequestBody();
        UpdateTrafficMirrorFilterOption trafficMirrorFilterbody = new UpdateTrafficMirrorFilterOption();
        trafficMirrorFilterbody.withDescription("description")
            .withName("test1");
        body.withTrafficMirrorFilter(trafficMirrorFilterbody);
        request.withBody(body);
        try {
            UpdateTrafficMirrorFilterResponse response = client.updateTrafficMirrorFilter(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

```
}  
}
```

Python

Change the name of the traffic mirror filter whose ID is 59d2b2e7-0d35-41f7-a12e-f7699366cd21 to test1.

```
# coding: utf-8  
  
import os  
from huaweicloudsdkcore.auth.credentials import BasicCredentials  
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion  
from huaweicloudsdkcore.exceptions import exceptions  
from huaweicloudsdkvpc.v3 import *  
  
if __name__ == "__main__":  
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security  
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment  
    # variables and decrypted during use to ensure security.  
    # In this example, AK and SK are stored in environment variables for authentication. Before running this  
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak = os.environ["CLOUD_SDK_AK"]  
    sk = os.environ["CLOUD_SDK_SK"]  
    projectId = "{project_id}"  
  
    credentials = BasicCredentials(ak, sk, projectId)  
  
    client = VpcClient.new_builder() \  
        .with_credentials(credentials) \  
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \  
        .build()  
  
    try:  
        request = UpdateTrafficMirrorFilterRequest()  
        request.traffic_mirror_filter_id = "{traffic_mirror_filter_id}"  
        trafficMirrorFilterbody = UpdateTrafficMirrorFilterOption(  
            description="description",  
            name="test1"  
        )  
        request.body = UpdateTrafficMirrorFilterRequestBody(  
            traffic_mirror_filter=trafficMirrorFilterbody  
        )  
        response = client.update_traffic_mirror_filter(request)  
        print(response)  
    except exceptions.ClientRequestException as e:  
        print(e.status_code)  
        print(e.request_id)  
        print(e.error_code)  
        print(e.error_msg)
```

Go

Change the name of the traffic mirror filter whose ID is 59d2b2e7-0d35-41f7-a12e-f7699366cd21 to test1.

```
package main  
  
import (  
    "fmt"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"  
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"  
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"  
)  
  
func main() {
```

```
// The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
// In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak := os.Getenv("CLOUD_SDK_AK")
sk := os.Getenv("CLOUD_SDK_SK")
projectId := "{project_id}"

auth := basic.NewCredentialsBuilder().
    WithAk(ak).
    WithSk(sk).
    WithProjectId(projectId).
    Build()

client := vpc.NewVpcClient(
    vpc.VpcClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.UpdateTrafficMirrorFilterRequest{
    request.TrafficMirrorFilterId = "{traffic_mirror_filter_id}"
    descriptionTrafficMirrorFilter:= "description"
    nameTrafficMirrorFilter:= "test1"
    trafficMirrorFilterbody := &model.UpdateTrafficMirrorFilterOption{
        Description: &descriptionTrafficMirrorFilter,
        Name: &nameTrafficMirrorFilter,
    }
    request.Body = &model.UpdateTrafficMirrorFilterRequestBody{
        TrafficMirrorFilter: trafficMirrorFilterbody,
    }
    response, err := client.UpdateTrafficMirrorFilter(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

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.

Calling Method

For details, see [Calling APIs](#).

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. For details about how to obtain a project ID, see Obtaining a Project ID .
traffic_mirror_filter_id	Yes	String	Traffic mirror filter ID.

Request Parameters

None

Response Parameters

Status code: 204

No Content

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

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
```

```
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class DeleteTrafficMirrorFilterSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();

        DeleteTrafficMirrorFilterRequest request = new DeleteTrafficMirrorFilterRequest();
        request.withTrafficMirrorFilterId("{traffic_mirror_filter_id}");
        try {
            DeleteTrafficMirrorFilterResponse response = client.deleteTrafficMirrorFilter(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
```

```
.with_region(VpcRegion.value_of("<YOUR REGION>")) \
.build()

try:
    request = DeleteTrafficMirrorFilterRequest()
    request.traffic_mirror_filter_id = "{traffic_mirror_filter_id}"
    response = client.delete_traffic_mirror_filter(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteTrafficMirrorFilterRequest{}
    request.TrafficMirrorFilterId = "{traffic_mirror_filter_id}"
    response, err := client.DeleteTrafficMirrorFilter(request)
    if err == nil {
        fmt.Printf("%v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

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 information about all traffic mirror filter rules, including the source and destination addresses and ports.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v3/{project_id}/vpc/traffic-mirror-filter-rules

Table 5-200 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: ID of the project that a traffic mirror filter rule belongs to. For details about how to obtain a project ID, see Obtaining a Project ID . Range: N/A

Table 5-201 Query Parameters

Parameter	Mandatory	Type	Description
id	No	Array of strings	Definition: ID of a traffic mirror filter rule. You can use this field to accurately filter traffic mirror filter rules. Multiple IDs can be specified for filtering. Range: N/A
action	No	Array of strings	Definition: Action of a traffic mirror filter rule. You can use this field to filter traffic mirror filter rules. Multiple actions can be specified for filtering. Range: accept and reject
description	No	Array of strings	Definition: Description of a traffic mirror filter rule. You can use this field to filter traffic mirror filter rules. Multiple descriptions can be specified for filtering. Range: N/A
destination_cidr_block	No	Array of strings	Definition: Destination of a traffic mirror filter rule. You can use this field to filter traffic mirror filter rules. Multiple destinations can be specified for filtering. Range: N/A

Parameter	Mandatory	Type	Description
destination_port_range	No	Array of strings	Definition: Destination port range of a traffic mirror filter rule. You can use this field to filter traffic mirror filter rules. Multiple destination port ranges can be specified for filtering. Range: N/A
direction	No	Array of strings	Definition: Direction of a traffic mirror filter rule. You can use this field to filter traffic mirror filter rules. Multiple directions can be specified for filtering. Range: • ingress: inbound traffic • egress: outbound traffic
priority	No	Array of integers	Definition: Priority of a traffic mirror filter rule. You can use this field to filter traffic mirror filter rules. Multiple priorities can be specified for filtering. Range: 1 to 65535

Parameter	Mandatory	Type	Description
protocol	No	Array of strings	Definition: Network protocol in a traffic mirror filter rule. You can use this field to filter traffic mirror filter rules. Multiple protocols can be specified for filtering. Range: • TCP: Traffic mirror rules with protocol set to TCP will be filtered. • UDP: Traffic mirror rules with protocol set to UDP will be filtered. • ICMP: Traffic mirror rules with protocol set to ICMP will be filtered. • ICMPV6: Traffic mirror rules with protocol set to ICMPv6 will be filtered. • ALL: Traffic mirror rules with protocol set to All will be filtered.
source_cidr_block	No	Array of strings	Definition: Source of a traffic mirror filter rule. You can use this field to filter traffic mirror filter rules. Multiple sources can be specified for filtering. Range: N/A
source_port_range	No	Array of strings	Definition: Source port range of a traffic mirror filter rule. You can use this field to filter traffic mirror filter rules. Multiple source port ranges can be specified for filtering. Range: N/A

Parameter	Mandatory	Type	Description
traffic_mirror_filter_id	No	Array of strings	Definition: ID of the traffic mirror filter that a traffic mirror filter rule belongs to. You can use this field to filter traffic mirror filter rules. Multiple IDs can be specified for filtering. Range: N/A

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	Definition: Response body for querying traffic mirror filter rules. Range: N/A
page_info	PageInfo object	Definition: Pagination information. Range: N/A
request_id	String	Definition: Request ID. Range: N/A

Table 5-203 TrafficMirrorFilterRule

Parameter	Type	Description
id	String	Definition: ID of a traffic mirror filter rule. Range: N/A
project_id	String	Definition: ID of the project that a traffic mirror filter rule belongs to. Range: N/A
description	String	Definition: Description of a traffic mirror filter rule. Range: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >).
traffic_mirror_filter_id	String	Definition: ID of the traffic mirror filter that a traffic mirror filter rule belongs to. Range: N/A
direction	String	Definition: Traffic direction of a traffic mirror filter rule. Range: • ingress: inbound traffic • egress: outbound traffic

Parameter	Type	Description
source_cidr_block	String	Definition: Source of a traffic mirror filter rule. Range: • Single IP address: IP address/subnet mask. For example, 192.168.10.10/32 for a single IPv4 address or 2002:50::44/128 for a single IPv6 address. • CIDR block: IP address/subnet mask. For example, 192.168.52.0/24 for an IPv4 CIDR block or 2407:c080:802:469::/64 for an IPv6 CIDR block. • All IP addresses: 0.0.0.0/0 indicates all IPv4 addresses, and ::/0 indicates all IPv6 addresses.
destination_cidr_block	String	Definition: Destination of a traffic mirror filter rule. Range: • Single IP address: IP address/subnet mask. For example, 192.168.10.10/32 for a single IPv4 address or 2002:50::44/128 for a single IPv6 address. • CIDR block: IP address/subnet mask. For example, 192.168.52.0/24 for an IPv4 CIDR block or 2407:c080:802:469::/64 for an IPv6 CIDR block. • All IP addresses: 0.0.0.0/0 indicates all IPv4 addresses, and ::/0 indicates all IPv6 addresses.
source_port_range	String	Definition: Source port range of a traffic mirror filter rule. Range: • Port range: 1 to 65535 • Use a hyphen (-) to connect the start port and the end port, for example, 22-23. The end port cannot be smaller than the start port.

Parameter	Type	Description
destination_port_range	String	Definition: Destination port range of a traffic mirror filter rule. Range: - Port range: 1 to 65535 - Use a hyphen (-) to connect the start port and the end port, for example, 22-23. The end port cannot be smaller than the start port.
ethertype	String	Definition: IP address version. Range: IPv4 or IPv6
protocol	String	Definition: Network protocol type. Range: TCP: If you select TCP, you can customize the source and destination port ranges. UDP: If you select UDP, you can customize the source and destination port ranges. ICMP: If you set IP address version to IPv4 and select ICMP, all ports are specified for source and destination port ranges by default. ICMPV6: If you set IP address version to IPv6 and select ICMPv6, all ports are specified for source and destination port ranges by default. ALL: If you select ALL, all network protocols are supported and all ports are specified for source and destination port ranges by default.
action	String	Definition: Action of a traffic mirror filter rule. Range: accept reject

Parameter	Type	Description
priority	Integer	Definition: Priority of a traffic mirror filter rule. Range: The value is from 1 to 65535. A smaller value indicates a higher priority.
created_at	String	Definition: Time when a traffic mirror filter rule was created. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .
updated_at	String	Definition: Time when a traffic mirror filter rule was updated. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .

Table 5-204 PageInfo

Parameter	Type	Description
previous_marker	String	Definition: The first record on the current page. Range: N/A
current_count	Integer	Definition: Total number of resources on the current page. Range: N/A
next_marker	String	Definition: The last record on the current page. The next_marker field does not exist if the page is the last one. Range: N/A

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
  } ],
  "page_info" : {
    "previous_marker" : "3daa97b5-ad58-477d-86a5-52b65257f94b",
    "current_count" : 1
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class ListTrafficMirrorFilterRulesSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
```

```
.withSk(sk);

VpcClient client = VpcClient.newBuilder()
    .withCredential(auth)
    .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
    .build();
ListTrafficMirrorFilterRulesRequest request = new ListTrafficMirrorFilterRulesRequest();
try {
    ListTrafficMirrorFilterRulesResponse response = client.listTrafficMirrorFilterRules(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListTrafficMirrorFilterRulesRequest()
        response = client.list_traffic_mirror_filter_rules(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
```

```
"github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListTrafficMirrorFilterRulesRequest{}
    response, err := client.ListTrafficMirrorFilterRules(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

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 information about a traffic mirror filter rule, including the source and destination addresses and ports.

Calling Method

For details, see [Calling APIs](#).

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	Definition: ID of the project that a traffic mirror filter rule belongs to. For details about how to obtain a project ID, see Obtaining a Project ID . Range: N/A
traffic_mirror_filter_rule_id	Yes	String	Definition: ID of a traffic mirror filter rule. You can call the API Querying Traffic Mirror Filter Rules to obtain the ID of the target traffic mirror filter rule, and then use this API to query details about the traffic mirror filter rule. Range: N/A

Request Parameters

None

Response Parameters

Status code: 200

Table 5-206 Response body parameters

Parameter	Type	Description
traffic_mirror_filter_rule	TrafficMirrorFilterRule object	Definition: Response body for querying details about a traffic mirror filter rule. Range: N/A
request_id	String	Definition: Request ID. Range: N/A

Table 5-207 TrafficMirrorFilterRule

Parameter	Type	Description
id	String	Definition: ID of a traffic mirror filter rule. Range: N/A
project_id	String	Definition: ID of the project that a traffic mirror filter rule belongs to. Range: N/A
description	String	Definition: Description of a traffic mirror filter rule. Range: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >).
traffic_mirror_filter_id	String	Definition: ID of the traffic mirror filter that a traffic mirror filter rule belongs to. Range: N/A

Parameter	Type	Description
direction	String	Definition: Traffic direction of a traffic mirror filter rule. Range: • ingress: inbound traffic • egress: outbound traffic
source_cidr_block	String	Definition: Source of a traffic mirror filter rule. Range: • Single IP address: IP address/subnet mask. For example, 192.168.10.10/32 for a single IPv4 address or 2002:50::44/128 for a single IPv6 address. • CIDR block: IP address/subnet mask. For example, 192.168.52.0/24 for an IPv4 CIDR block or 2407:c080:802:469::/64 for an IPv6 CIDR block. • All IP addresses: 0.0.0.0/0 indicates all IPv4 addresses, and ::/0 indicates all IPv6 addresses.
destination_cidr_block	String	Definition: Destination of a traffic mirror filter rule. Range: • Single IP address: IP address/subnet mask. For example, 192.168.10.10/32 for a single IPv4 address or 2002:50::44/128 for a single IPv6 address. • CIDR block: IP address/subnet mask. For example, 192.168.52.0/24 for an IPv4 CIDR block or 2407:c080:802:469::/64 for an IPv6 CIDR block. • All IP addresses: 0.0.0.0/0 indicates all IPv4 addresses, and ::/0 indicates all IPv6 addresses.

Parameter	Type	Description
source_port_range	String	Definition: Source port range of a traffic mirror filter rule. Range: - Port range: 1 to 65535 - Use a hyphen (-) to connect the start port and the end port, for example, 22-23. The end port cannot be smaller than the start port.
destination_port_range	String	Definition: Destination port range of a traffic mirror filter rule. Range: - Port range: 1 to 65535 - Use a hyphen (-) to connect the start port and the end port, for example, 22-23. The end port cannot be smaller than the start port.
ethertype	String	Definition: IP address version. Range: IPv4 or IPv6

Parameter	Type	Description
protocol	String	Definition: Network protocol type. Range: • TCP: If you select TCP, you can customize the source and destination port ranges. • UDP: If you select UDP, you can customize the source and destination port ranges. • ICMP: If you set IP address version to IPv4 and select ICMP, all ports are specified for source and destination port ranges by default. • ICMPV6: If you set IP address version to IPv6 and select ICMPv6, all ports are specified for source and destination port ranges by default. • ALL: If you select ALL, all network protocols are supported and all ports are specified for source and destination port ranges by default.
action	String	Definition: Action of a traffic mirror filter rule. Range: • accept • reject
priority	Integer	Definition: Priority of a traffic mirror filter rule. Range: The value is from 1 to 65535. A smaller value indicates a higher priority.
created_at	String	Definition: Time when a traffic mirror filter rule was created. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .

Parameter	Type	Description
updated_at	String	Definition: Time when a traffic mirror filter rule was updated. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .

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" : "8.8.8/32",
    "destination_cidr_block" : "9.9.9/32",
    "destination_port_range" : "10-65535",
    "action" : "accept",
    "priority" : 20
  },
  "request_id" : "ca9682cf-0680-469f-bb04-5b0f17b075d0"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;
```

```
public class ShowTrafficMirrorFilterRuleSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();
        ShowTrafficMirrorFilterRuleRequest request = new ShowTrafficMirrorFilterRuleRequest();
        request.withTrafficMirrorFilterRuleId("{traffic_mirror_filter_rule_id}");
        try {
            ShowTrafficMirrorFilterRuleResponse response = client.showTrafficMirrorFilterRule(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.getenv("CLOUD_SDK_AK")
    sk = os.getenv("CLOUD_SDK_SK")
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
```

```
request = ShowTrafficMirrorFilterRuleRequest()
request.traffic_mirror_filter_rule_id = "{traffic_mirror_filter_rule_id}"
response = client.show_traffic_mirror_filter_rule(request)
print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowTrafficMirrorFilterRuleRequest{
        request.TrafficMirrorFilterRuleId = "{traffic_mirror_filter_rule_id}"
    }
    response, err := client.ShowTrafficMirrorFilterRule(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

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.

Calling Method

For details, see [Calling APIs](#).

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. For details about how to obtain a project ID, see Obtaining a 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	Definition: Response body for querying details about a traffic mirror filter rule. Range: N/A
request_id	String	Definition: Request ID. Range: N/A

Table 5-212 TrafficMirrorFilterRule

Parameter	Type	Description
id	String	Definition: ID of a traffic mirror filter rule. Range: N/A
project_id	String	Definition: ID of the project that a traffic mirror filter rule belongs to. Range: N/A
description	String	Definition: Description of a traffic mirror filter rule. Range: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >).
traffic_mirror_filter_id	String	Definition: ID of the traffic mirror filter that a traffic mirror filter rule belongs to. Range: N/A

Parameter	Type	Description
direction	String	Definition: Traffic direction of a traffic mirror filter rule. Range: • ingress: inbound traffic • egress: outbound traffic
source_cidr_block	String	Definition: Source of a traffic mirror filter rule. Range: • Single IP address: IP address/subnet mask. For example, 192.168.10.10/32 for a single IPv4 address or 2002:50::44/128 for a single IPv6 address. • CIDR block: IP address/subnet mask. For example, 192.168.52.0/24 for an IPv4 CIDR block or 2407:c080:802:469::/64 for an IPv6 CIDR block. • All IP addresses: 0.0.0.0/0 indicates all IPv4 addresses, and ::/0 indicates all IPv6 addresses.
destination_cidr_block	String	Definition: Destination of a traffic mirror filter rule. Range: • Single IP address: IP address/subnet mask. For example, 192.168.10.10/32 for a single IPv4 address or 2002:50::44/128 for a single IPv6 address. • CIDR block: IP address/subnet mask. For example, 192.168.52.0/24 for an IPv4 CIDR block or 2407:c080:802:469::/64 for an IPv6 CIDR block. • All IP addresses: 0.0.0.0/0 indicates all IPv4 addresses, and ::/0 indicates all IPv6 addresses.

Parameter	Type	Description
source_port_range	String	Definition: Source port range of a traffic mirror filter rule. Range: - Port range: 1 to 65535 - Use a hyphen (-) to connect the start port and the end port, for example, 22-23. The end port cannot be smaller than the start port.
destination_port_range	String	Definition: Destination port range of a traffic mirror filter rule. Range: - Port range: 1 to 65535 - Use a hyphen (-) to connect the start port and the end port, for example, 22-23. The end port cannot be smaller than the start port.
ethertype	String	Definition: IP address version. Range: IPv4 or IPv6

Parameter	Type	Description
protocol	String	Definition: Network protocol type. Range: • TCP: If you select TCP, you can customize the source and destination port ranges. • UDP: If you select UDP, you can customize the source and destination port ranges. • ICMP: If you set IP address version to IPv4 and select ICMP, all ports are specified for source and destination port ranges by default. • ICMPV6: If you set IP address version to IPv6 and select ICMPv6, all ports are specified for source and destination port ranges by default. • ALL: If you select ALL, all network protocols are supported and all ports are specified for source and destination port ranges by default.
action	String	Definition: Action of a traffic mirror filter rule. Range: • accept • reject
priority	Integer	Definition: Priority of a traffic mirror filter rule. Range: The value is from 1 to 65535. A smaller value indicates a higher priority.
created_at	String	Definition: Time when a traffic mirror filter rule was created. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .

Parameter	Type	Description
updated_at	String	Definition: Time when a traffic mirror filter rule was updated. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .

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
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

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.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class CreateTrafficMirrorFilterRuleSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();
        CreateTrafficMirrorFilterRuleRequest request = new CreateTrafficMirrorFilterRuleRequest();
        CreateTrafficMirrorFilterRuleRequestBody body = new CreateTrafficMirrorFilterRuleRequestBody();
        CreateTrafficMirrorFilterRuleOption trafficMirrorFilterRulebody = new
        CreateTrafficMirrorFilterRuleOption();
        trafficMirrorFilterRulebody.withTrafficMirrorFilterId("417d7317-6c17-4428-a0f3-997d3e2293a0")
            .withDirection("ingress")
            .withProtocol("ICMP")
            .withEthertype("ipv4")
            .withSourceCidrBlock("192.168.0.0/24")
            .withAction("accept")
            .withPriority(29);
        body.withTrafficMirrorFilterRule(trafficMirrorFilterRulebody);
        request.withBody(body);
        try {
            CreateTrafficMirrorFilterRuleResponse response = client.createTrafficMirrorFilterRule(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

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.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateTrafficMirrorFilterRuleRequest()
        trafficMirrorFilterRulebody = CreateTrafficMirrorFilterRuleOption(
            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
        )
        request.body = CreateTrafficMirrorFilterRuleRequestBody(
            traffic_mirror_filter_rule=trafficMirrorFilterRulebody
        )
        response = client.create_traffic_mirror_filter_rule(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

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.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
```

```
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateTrafficMirrorFilterRuleRequest{}
    sourceCidrBlockTrafficMirrorFilterRule := "192.168.0.0/24"
    trafficMirrorFilterRulebody := &model.CreateTrafficMirrorFilterRuleOption{
        TrafficMirrorFilterId: "417d7317-6c17-4428-a0f3-997d3e2293a0",
        Direction: "ingress",
        Protocol: "ICMP",
        Ethertype: "ipv4",
        SourceCidrBlock: &sourceCidrBlockTrafficMirrorFilterRule,
        Action: "accept",
        Priority: int32(29),
    }
    request.Body = &model.CreateTrafficMirrorFilterRuleRequestBody{
        TrafficMirrorFilterRule: trafficMirrorFilterRulebody,
    }
    response, err := client.CreateTrafficMirrorFilterRule(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

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.

Calling Method

For details, see [Calling APIs](#).

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. For details about how to obtain a project ID, see Obtaining a 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 >).

Parameter	Mandatory	Type	Description
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	Destination 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	Definition: Response body for querying details about a traffic mirror filter rule. Range: N/A

Parameter	Type	Description
request_id	String	Definition: Request ID. Range: N/A

Table 5-217 TrafficMirrorFilterRule

Parameter	Type	Description
id	String	Definition: ID of a traffic mirror filter rule. Range: N/A
project_id	String	Definition: ID of the project that a traffic mirror filter rule belongs to. Range: N/A
description	String	Definition: Description of a traffic mirror filter rule. Range: The value can contain 0 to 255 characters and cannot contain angle brackets (< or >).
traffic_mirror_filter_id	String	Definition: ID of the traffic mirror filter that a traffic mirror filter rule belongs to. Range: N/A
direction	String	Definition: Traffic direction of a traffic mirror filter rule. Range: • ingress: inbound traffic • egress: outbound traffic

Parameter	Type	Description
source_cidr_block	String	Definition: Source of a traffic mirror filter rule. Range: • Single IP address: IP address/subnet mask. For example, 192.168.10.10/32 for a single IPv4 address or 2002:50::44/128 for a single IPv6 address. • CIDR block: IP address/subnet mask. For example, 192.168.52.0/24 for an IPv4 CIDR block or 2407:c080:802:469::/64 for an IPv6 CIDR block. • All IP addresses: 0.0.0.0/0 indicates all IPv4 addresses, and ::/0 indicates all IPv6 addresses.
destination_cidr_block	String	Definition: Destination of a traffic mirror filter rule. Range: • Single IP address: IP address/subnet mask. For example, 192.168.10.10/32 for a single IPv4 address or 2002:50::44/128 for a single IPv6 address. • CIDR block: IP address/subnet mask. For example, 192.168.52.0/24 for an IPv4 CIDR block or 2407:c080:802:469::/64 for an IPv6 CIDR block. • All IP addresses: 0.0.0.0/0 indicates all IPv4 addresses, and ::/0 indicates all IPv6 addresses.
source_port_range	String	Definition: Source port range of a traffic mirror filter rule. Range: • Port range: 1 to 65535 • Use a hyphen (-) to connect the start port and the end port, for example, 22-23. The end port cannot be smaller than the start port.

Parameter	Type	Description
destination_port_range	String	Definition: Destination port range of a traffic mirror filter rule. Range: - Port range: 1 to 65535 - Use a hyphen (-) to connect the start port and the end port, for example, 22-23. The end port cannot be smaller than the start port.
ethertype	String	Definition: IP address version. Range: IPv4 or IPv6
protocol	String	Definition: Network protocol type. Range: TCP: If you select TCP, you can customize the source and destination port ranges. UDP: If you select UDP, you can customize the source and destination port ranges. ICMP: If you set IP address version to IPv4 and select ICMP, all ports are specified for source and destination port ranges by default. ICMPV6: If you set IP address version to IPv6 and select ICMPv6, all ports are specified for source and destination port ranges by default. ALL: If you select ALL, all network protocols are supported and all ports are specified for source and destination port ranges by default.
action	String	Definition: Action of a traffic mirror filter rule. Range: accept reject

Parameter	Type	Description
priority	Integer	Definition: Priority of a traffic mirror filter rule. Range: The value is from 1 to 65535. A smaller value indicates a higher priority.
created_at	String	Definition: Time when a traffic mirror filter rule was created. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .
updated_at	String	Definition: Time when a traffic mirror filter rule was updated. Range: The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i> .

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
}
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Change action of the traffic mirror filter rule whose ID is 7c12805a-1b8d-40b5-ab23-a8fac480f2ec to reject.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class UpdateTrafficMirrorFilterRuleSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();

        UpdateTrafficMirrorFilterRuleRequest request = new UpdateTrafficMirrorFilterRuleRequest();
        request.withTrafficMirrorFilterRuleId("{traffic_mirror_filter_rule_id}");
        UpdateTrafficMirrorFilterRuleRequestBody body = new UpdateTrafficMirrorFilterRuleRequestBody();
        UpdateTrafficMirrorFilterRuleOption trafficMirrorFilterRulebody = new
        UpdateTrafficMirrorFilterRuleOption();
        trafficMirrorFilterRulebody.withSourceCidrBlock("10.0.0.0/8")
            .withDestinationCidrBlock("192.168.1.0/24")
            .withSourcePortRange("80-90")
            .withAction("reject");
        body.withTrafficMirrorFilterRule(trafficMirrorFilterRulebody);
        request.withBody(body);
        try {
            UpdateTrafficMirrorFilterRuleResponse response = client.updateTrafficMirrorFilterRule(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
```

```
        e.printStackTrace();
    } catch (RequestTimeoutException e) {
        e.printStackTrace();
    } catch (ServiceResponseException e) {
        e.printStackTrace();
        System.out.println(e.getHttpStatusCode());
        System.out.println(e.getRequestId());
        System.out.println(e.getErrorCode());
        System.out.println(e.getErrorMsg());
    }
}
}
```

Python

Change action of the traffic mirror filter rule whose ID is 7c12805a-1b8d-40b5-ab23-a8fac480f2ec to reject.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdateTrafficMirrorFilterRuleRequest()
        request.traffic_mirror_filter_rule_id = "{traffic_mirror_filter_rule_id}"
        trafficMirrorFilterRulebody = UpdateTrafficMirrorFilterRuleOption(
            source_cidr_block="10.0.0.0/8",
            destination_cidr_block="192.168.1.0/24",
            source_port_range="80-90",
            action="reject"
        )
        request.body = UpdateTrafficMirrorFilterRuleRequestBody(
            traffic_mirror_filter_rule=trafficMirrorFilterRulebody
        )
        response = client.update_traffic_mirror_filter_rule(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Change action of the traffic mirror filter rule whose ID is 7c12805a-1b8d-40b5-ab23-a8fac480f2ec to reject.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdateTrafficMirrorFilterRuleRequest{}
    request.TrafficMirrorFilterRuleId = "{traffic_mirror_filter_rule_id}"
    sourceCidrBlockTrafficMirrorFilterRule := "10.0.0.0/8"
    destinationCidrBlockTrafficMirrorFilterRule := "192.168.1.0/24"
    sourcePortRangeTrafficMirrorFilterRule := "80-90"
    actionTrafficMirrorFilterRule := "reject"
    trafficMirrorFilterRulebody := &model.UpdateTrafficMirrorFilterRuleOption{
        SourceCidrBlock: &sourceCidrBlockTrafficMirrorFilterRule,
        DestinationCidrBlock: &destinationCidrBlockTrafficMirrorFilterRule,
        SourcePortRange: &sourcePortRangeTrafficMirrorFilterRule,
        Action: &actionTrafficMirrorFilterRule,
    }
    request.Body = &model.UpdateTrafficMirrorFilterRuleRequestBody{
        TrafficMirrorFilterRule: trafficMirrorFilterRulebody,
    }
    response, err := client.UpdateTrafficMirrorFilterRule(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

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.

Calling Method

For details, see [Calling APIs](#).

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. For details about how to obtain a project ID, see Obtaining a Project ID .
traffic_mirror_filter_rule_id	Yes	String	Traffic mirror filter rule ID.

Request Parameters

None

Response Parameters

Status code: 204

No Content

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

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class DeleteTrafficMirrorFilterRuleSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();

        DeleteTrafficMirrorFilterRuleRequest request = new DeleteTrafficMirrorFilterRuleRequest();
        request.withTrafficMirrorFilterRuleId("{traffic_mirror_filter_rule_id}");
        try {
            DeleteTrafficMirrorFilterRuleResponse response = client.deleteTrafficMirrorFilterRule(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrMsg());
        }
    }
}
```



```
}  
}
```

Python

```
# coding: utf-8  
  
import os  
from huaweicloudsdkcore.auth.credentials import BasicCredentials  
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion  
from huaweicloudsdkcore.exceptions import exceptions  
from huaweicloudsdkvpc.v3 import *  
  
if __name__ == "__main__":  
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security  
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment  
    # variables and decrypted during use to ensure security.  
    # In this example, AK and SK are stored in environment variables for authentication. Before running this  
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak = os.environ["CLOUD_SDK_AK"]  
    sk = os.environ["CLOUD_SDK_SK"]  
    projectId = "{project_id}"  
  
    credentials = BasicCredentials(ak, sk, projectId)  
  
    client = VpcClient.new_builder() \  
        .with_credentials(credentials) \  
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \  
        .build()  
  
    try:  
        request = DeleteTrafficMirrorFilterRuleRequest()  
        request.traffic_mirror_filter_rule_id = "{traffic_mirror_filter_rule_id}"  
        response = client.delete_traffic_mirror_filter_rule(request)  
        print(response)  
    except exceptions.ClientRequestException as e:  
        print(e.status_code)  
        print(e.request_id)  
        print(e.error_code)  
        print(e.error_msg)
```

Go

```
package main  
  
import (  
    "fmt"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"  
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"  
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"  
)  
  
func main() {  
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security  
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment  
    // variables and decrypted during use to ensure security.  
    // In this example, AK and SK are stored in environment variables for authentication. Before running this  
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak := os.Getenv("CLOUD_SDK_AK")  
    sk := os.Getenv("CLOUD_SDK_SK")  
    projectId := "{project_id}"  
  
    auth := basic.NewCredentialsBuilder().  
        WithAk(ak).  
        WithSk(sk).  
        WithProjectId(projectId).  
        Build()
```

```
client := vpc.NewVpcClient(  
    vpc.VpcClientBuilder().  
        WithRegion(region.ValueOf("<YOUR REGION>")).  
        WithCredential(auth).  
        Build())  
  
request := &model.DeleteTrafficMirrorFilterRuleRequest{  
    request.TrafficMirrorFilterRuleId = "{traffic_mirror_filter_rule_id}"  
    response, err := client.DeleteTrafficMirrorFilterRule(request)  
    if err == nil {  
        fmt.Printf("%v\n", response)  
    } else {  
        fmt.Println(err)  
    }  
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
204	No Content

Error Codes

See [Error Codes](#).

5.9 Network ACL

5.9.1 Creating a Network ACL

Function

This API is used to create a network ACL.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v3/{project_id}/vpc/firewalls

Table 5-219 Path Parameters

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 5-220 Request body parameters

Parameter	Mandatory	Type	Description
firewall	Yes	CreateFirewallOption object	Request body for creating a network ACL.
dry_run	No	Boolean	- Whether to only send the check request. - The value can be one of the following: true: A check request will be sent and the network ACL will not be created. Check items include mandatory parameters, request format, and constraints. 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 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	- Description about the network ACL. - The value can contain no more than 255 characters. - The value cannot contain angle brackets (< or >).
enterprise_project_id	No	String	- ID of the enterprise project that is associated with the network ACL. - The project ID can be 0 or a string that contains a maximum of 36 characters in UUID format with hyphens (-). 0 indicates the default enterprise project.
tags	No	Array of ResourceTag objects	Network ACL resource tags.
admin_state_up	No	Boolean	- Whether a network ACL is enabled. The default value is true. - The value can be true (enabled) or false (disabled).

Table 5-222 ResourceTag

Parameter	Mandatory	Type	Description
key	Yes	String	- Tag key - Tag keys must be unique for each resource. - The value can contain 1 to 128 characters. Minimum: 1 Maximum: 128

Parameter	Mandatory	Type	Description
value	Yes	String	- Tag value. - The value can contain no more than 255 characters Maximum: 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	- The unique ID of 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	- Description about the network ACL. - The value can contain no more than 255 characters. - The value cannot contain angle brackets (< or >).
project_id	String	ID of the project that is associated with the network ACL.

Parameter	Type	Description
created_at	String	- Time when the network ACL was created. - The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ss</i>, which is automatically generated by the system.
updated_at	String	- Time when the network ACL was last updated. - The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ss</i>, which is automatically generated by the system.
admin_state_up	Boolean	- Whether a network ACL is enabled. - The value can be true (enabled) or false (disabled).
status	String	Network ACL status.
enterprise_project_id	String	- ID of the enterprise project that is associated with the network ACL. - The project ID can be 0 or a string that contains a maximum of 36 characters in UUID format with hyphens (-). 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 5-225 ResourceTag

Parameter	Type	Description
key	String	- Tag key - Tag keys must be unique for each resource. - The value can contain 1 to 128 characters. Minimum: 1 Maximum: 128
value	String	- Tag value. - The value can contain no more than 255 characters Maximum: 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 (.).
description	String	- Description about the 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. allow indicates traffic is allowed and deny indicates that traffic is denied.
project_id	String	ID of the project that is associated with a network ACL rule.
protocol	String	- Network ACL rule protocol. - The value can be tcp, udp, icmp, icmpv6, or an IP protocol number (0-255).
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 specified 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 specified 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 maximum number of port entries is 20 by default.
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 maximum number of port entries is 20 by default.

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 specified 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 specified at the same time.
enabled	Boolean	- Whether to enable a network ACL rule. true means to enable the network ACL rule and false means to disable the network ACL rule. - The default value is true.

Example Requests

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 Responses

Status code: 201

Normal response to the POST operation. For more status codes, see [Status Codes](#).

```
{
  "firewall": {
    "id": "e9a7731d-5bd9-4250-a524-b9a076fd5629",
    "name": "network_acl_test1",
    "description": "network_acl_test1",
    "project_id": "9476ea5a8a9849c38358e43c0c3a9e12",
    "created_at": "2022-04-07T07:30:46.000+00:00",
    "updated_at": "2022-04-07T07:30:46.000+00:00",
    "admin_state_up": true,
    "enterprise_project_id": "158ad39a-dab7-45a3-9b5a-2836b3cf93f9",
    "status": "ACTIVE",
    "tags": [],
    "ingress_rules": [],
    "egress_rules": [],
    "associations": []
  }
}
```

```
}  
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Create a network ACL named **network_acl_test1**.

```
package com.huaweicloud.sdk.test;  
  
import com.huaweicloud.sdk.core.auth.ICredential;  
import com.huaweicloud.sdk.core.auth.BasicCredentials;  
import com.huaweicloud.sdk.core.exception.ConnectionException;  
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;  
import com.huaweicloud.sdk.core.exception.ServiceResponseException;  
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;  
import com.huaweicloud.sdk.vpc.v3.*;  
import com.huaweicloud.sdk.vpc.v3.model.*;  
  
public class CreateFirewallSolution {  
  
    public static void main(String[] args) {  
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great  
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or  
        // environment variables and decrypted during use to ensure security.  
        // In this example, AK and SK are stored in environment variables for authentication. Before running  
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
        String ak = System.getenv("CLOUD_SDK_AK");  
        String sk = System.getenv("CLOUD_SDK_SK");  
        String projectId = "{project_id}";  
  
        ICredential auth = new BasicCredentials()  
            .withProjectId(projectId)  
            .withAk(ak)  
            .withSk(sk);  
  
        VpcClient client = VpcClient.newBuilder()  
            .withCredential(auth)  
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))  
            .build();  
        CreateFirewallRequest request = new CreateFirewallRequest();  
        CreateFirewallRequestBody body = new CreateFirewallRequestBody();  
        CreateFirewallOption firewallbody = new CreateFirewallOption();  
        firewallbody.withName("network_acl_test1")  
            .withDescription("network_acl_test1")  
            .withEnterpriseProjectId("158ad39a-dab7-45a3-9b5a-2836b3cf93f9");  
        body.withFirewall(firewallbody);  
        request.withBody(body);  
        try {  
            CreateFirewallResponse response = client.createFirewall(request);  
            System.out.println(response.toString());  
        } catch (ConnectionException e) {  
            e.printStackTrace();  
        } catch (RequestTimeoutException e) {  
            e.printStackTrace();  
        } catch (ServiceResponseException e) {  
            e.printStackTrace();  
            System.out.println(e.getHttpStatusCode());  
            System.out.println(e.getRequestId());  
            System.out.println(e.getErrorCode());  
            System.out.println(e.getErrorMsg());  
        }  
    }  
}
```

Python

Create a network ACL named **network_acl_test1**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateFirewallRequest()
        firewallbody = CreateFirewallOption(
            name="network_acl_test1",
            description="network_acl_test1",
            enterprise_project_id="158ad39a-dab7-45a3-9b5a-2836b3cf93f9"
        )
        request.body = CreateFirewallRequestBody(
            firewall=firewallbody
        )
        response = client.create_firewall(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Create a network ACL named **network_acl_test1**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
```

```
sk := os.Getenv("CLOUD_SDK_SK")
projectId := "{project_id}"

auth := basic.NewCredentialsBuilder().
    WithAk(ak).
    WithSk(sk).
    WithProjectId(projectId).
    Build()

client := vpc.NewVpcClient(
    vpc.VpcClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.CreateFirewallRequest{}
descriptionFirewall:= "network_acl_test1"
enterpriseProjectIdFirewall:= "158ad39a-dab7-45a3-9b5a-2836b3cf93f9"
firewallbody := &model.CreateFirewallOption{
    Name: "network_acl_test1",
    Description: &descriptionFirewall,
    EnterpriseProjectId: &enterpriseProjectIdFirewall,
}
request.Body = &model.CreateFirewallRequestBody{
    Firewall: firewallbody,
}
response, err := client.CreateFirewall(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
201	Normal response to the POST operation. For more 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.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v3/{project_id}/vpc/firewalls

Table 5-228 Path Parameters

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 5-229 Query Parameters

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.
id	No	Array of strings	Unique ID of a network ACL, which is used to filter the network ACL. Multiple IDs can be specified for filtering.
name	No	Array of strings	Network ACL name, which is used to filter the network ACL. Multiple names can be specified for filtering.
status	No	String	Network ACL status, which is used to filter the network ACL.
admin_state_up	No	Boolean	Admin state of a network ACL, which is used to filter the network ACL.

Parameter	Mandatory	Type	Description
enterprise_project_id	No	Array of strings	- Enterprise project ID. This parameter is used to filter the network ACLs of an enterprise project. - The project ID can be 0 or a string that contains a maximum of 36 characters in UUID format with hyphens (-). 0 indicates the default enterprise project. To obtain network ACLs of all enterprise projects, set this parameter to all_granted_eps.

Request Parameters

None

Response Parameters

Status code: 200

Table 5-230 Response body parameters

Parameter	Type	Description
firewalls	Array of ListFirewallDetail objects	Response body for querying network ACLs.
page_info	PageInfo object	Pagination information.
request_id	String	Request ID.

Table 5-231 ListFirewallDetail

Parameter	Type	Description
id	String	- The unique ID of 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	- Description about the network ACL. - The value can contain no more than 255 characters. - The value cannot contain angle brackets (< or >).
project_id	String	ID of the project that is associated with the network ACL.
created_at	String	- Time when the network ACL was created. - The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ss</i>, which is automatically generated by the system.
updated_at	String	- Time when the network ACL was last updated. - The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ssZ</i>, which is automatically generated by the system.
admin_state_up	Boolean	- Whether a network ACL is enabled. - The value can be true (enabled) or false (disabled).
status	String	Network ACL status.
enterprise_project_id	String	- ID of the enterprise project that is associated with the network ACL. - The project ID can be 0 or a string that contains a maximum of 36 characters in UUID format with hyphens (-). 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. - The value can contain 1 to 128 characters. Minimum: 1 Maximum: 128
value	String	- Tag value. - The value can contain no more than 255 characters Maximum: 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	Definition: The first record on the current page. Range: N/A
current_count	Integer	Definition: Total number of resources on the current page. Range: N/A
next_marker	String	Definition: The last record on the current page. The next_marker field does not exist if the page is the last one. Range: N/A

Example Requests

Querying network ACLs

```
GET https://{Endpoint}/v3/{project_id}/vpc/firewalls
```

Example Responses

Status code: 200

Normal response to the GET operation. For more status codes, see [Status Codes](#).

```
{
  "firewalls" : [ {
    "id" : "e9a7731d-5bd9-4250-a524-b9a076fd5629",
    "name" : "network_acl_test1",
    "description" : "network_acl_test1",
    "project_id" : "9476ea5a8a9849c38358e43c0c3a9e12",
    "created_at" : "2022-04-07T07:30:46.000+00:00",
    "updated_at" : "2022-04-07T07:30:46.000+00:00",
    "admin_state_up" : true,
    "enterprise_project_id" : "158ad39a-dab7-45a3-9b5a-2836b3cf93f9",
    "status" : "ACTIVE",
    "tags" : [ ],
    "associations" : [ {
      "vsubnet_id" : "8359e5b0-353f-4ef3-a071-98e67a34a143"
    } ]
  } ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class ListFirewallSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
```

```
        .withCredential(auth)
        .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
        .build();
ListFirewallRequest request = new ListFirewallRequest();
try {
    ListFirewallResponse response = client.listFirewall(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListFirewallRequest()
        response = client.list_firewall(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)
```

```
func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListFirewallRequest{}
    response, err := client.ListFirewall(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Normal response to the GET operation. For more status codes, see Status Codes .

Error Codes

See [Error Codes](#).

5.9.3 Querying the Details of a Network ACL

Function

This API is used query the details of a network ACL.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v3/{project_id}/vpc/firewalls/{firewall_id}

Table 5-235 Path Parameters

Parameter	Mandatory	Type	Description
firewall_id	Yes	String	Unique ID of a network ACL.
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see Obtaining a 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	- The unique ID of 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 (.).

Parameter	Type	Description
description	String	• Description about the network ACL. • The value can contain no more than 255 characters. • The value cannot contain angle brackets (< or >).
project_id	String	• ID of the project that is associated with the network ACL.
created_at	String	• Time when the network ACL was created. • The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ss</i>, which is automatically generated by the system.
updated_at	String	• Time when the network ACL was last updated. • The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ss</i>, which is automatically generated by the system.
admin_state_up	Boolean	• Whether a network ACL is enabled. • The value can be true (enabled) or false (disabled).
status	String	• Network ACL status.
enterprise_project_id	String	• ID of the enterprise project that is associated with the network ACL. • The project ID can be 0 or a string that contains a maximum of 36 characters in UUID format with hyphens (-). 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. - The value can contain 1 to 128 characters. Minimum: 1 Maximum: 128
value	String	- Tag value. - The value can contain no more than 255 characters Maximum: 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 (.).

Parameter	Type	Description
description	String	• Description about the 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. • allow indicates traffic is allowed and deny indicates that traffic is denied.
project_id	String	• ID of the project that is associated with a network ACL rule.
protocol	String	• Network ACL rule protocol. • The value can be tcp, udp, icmp, icmpv6, or an IP protocol number (0-255).
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 specified 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 specified 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 maximum number of port entries is 20 by default.

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 maximum number of port entries is 20 by default.
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 specified 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 specified at the same time.
enabled	Boolean	- Whether to enable a network ACL rule. true means to enable the network ACL rule and false means to disable the network ACL rule. - The default value is true.

Example Requests

Querying the details of a network ACL

```
GET https://{Endpoint}/v3/{project_id}/vpc/firewalls/{firewall_id}
```

Example Responses

Status code: 200

Normal response to the GET operation. For more status codes, see [Status Codes](#).

```
{
  "firewall": {
    "id": "e9a7731d-5bd9-4250-a524-b9a076fd5629",
    "name": "network_acl_test1",
    "description": "network_acl_test1",
    "project_id": "9476ea5a8a9849c38358e43c0c3a9e12",
    "created_at": "2022-04-07T07:30:46.000+00:00",
    "updated_at": "2022-04-07T07:30:46.000+00:00",
    "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"
},
{
  "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"
},
{
  "associations": [ {
    "vsubnet_id": "8359e5b0-353f-4ef3-a071-98e67a34a143"
  } ]
}
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class ShowFirewallSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
```

```
        .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
        .build();
ShowFirewallRequest request = new ShowFirewallRequest();
request.withFirewallId("{firewall_id}");
try {
    ShowFirewallResponse response = client.showFirewall(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowFirewallRequest()
        request.firewall_id = "{firewall_id}"
        response = client.show_firewall(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
```

```
)  
  
func main() {  
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security  
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment  
    // variables and decrypted during use to ensure security.  
    // In this example, AK and SK are stored in environment variables for authentication. Before running this  
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak := os.Getenv("CLOUD_SDK_AK")  
    sk := os.Getenv("CLOUD_SDK_SK")  
    projectId := "{project_id}"  
  
    auth := basic.NewCredentialsBuilder().  
        WithAk(ak).  
        WithSk(sk).  
        WithProjectId(projectId).  
        Build()  
  
    client := vpc.NewVpcClient(  
        vpc.VpcClientBuilder().  
            WithRegion(region.ValueOf("<YOUR REGION>")).  
            WithCredential(auth).  
            Build())  
  
    request := &model.ShowFirewallRequest{  
        request.FirewallId = "{firewall_id}"  
    }  
    response, err := client.ShowFirewall(request)  
    if err == nil {  
        fmt.Printf("%+v\n", response)  
    } else {  
        fmt.Println(err)  
    }  
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Normal response to the GET operation. For more 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.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v3/{project_id}/vpc/firewalls/{firewall_id}

Table 5-241 Path Parameters

Parameter	Mandatory	Type	Description
firewall_id	Yes	String	Unique ID of a network ACL.
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see Obtaining a Project ID .

Request Parameters

Table 5-242 Request body parameters

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	- Description about the network ACL. - The value can contain no more than 255 characters. - The value cannot contain angle brackets (< or >).

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	- Whether a network ACL is enabled. - The value can be true (enabled) or false (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	- The unique ID of 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	- Description about the network ACL. - The value can contain no more than 255 characters. - The value cannot contain angle brackets (< or >).
project_id	String	ID of the project that is associated with the network ACL.

Parameter	Type	Description
created_at	String	- Time when the network ACL was created. - The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ss</i>, which is automatically generated by the system.
updated_at	String	- Time when the network ACL was last updated. - The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ss</i>, which is automatically generated by the system.
admin_state_up	Boolean	- Whether a network ACL is enabled. - The value can be true (enabled) or false (disabled).
status	String	Network ACL status.
enterprise_project_id	String	- ID of the enterprise project that is associated with the network ACL. - The project ID can be 0 or a string that contains a maximum of 36 characters in UUID format with hyphens (-). 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 5-246 ResourceTag

Parameter	Type	Description
key	String	- Tag key - Tag keys must be unique for each resource. - The value can contain 1 to 128 characters. Minimum: 1 Maximum: 128
value	String	- Tag value. - The value can contain no more than 255 characters Maximum: 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 (.).
description	String	- Description about the 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. allow indicates traffic is allowed and deny indicates that traffic is denied.
project_id	String	ID of the project that is associated with a network ACL rule.
protocol	String	- Network ACL rule protocol. - The value can be tcp, udp, icmp, icmpv6, or an IP protocol number (0-255).
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 specified 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 specified 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 maximum number of port entries is 20 by default.
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 maximum number of port entries is 20 by default.

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 specified 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 specified at the same time.
enabled	Boolean	- Whether to enable a network ACL rule. true means to enable the network ACL rule and false means to disable the network ACL rule. - The default value is true.

Example Requests

Change the name and description of the network ACL whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5629** to **network_acl_test1** and enable the network ACL.

```
PUT https://{Endpoint}/v3/9476ea5a8a9849c38358e43c0c3a9e12/vpc/firewalls/e9a7731d-5bd9-4250-a524-b9a076fd5629
```

```
{
  "firewall" : {
    "name" : "network_acl_test1",
    "description" : "network_acl_test1",
    "admin_state_up" : true
  }
}
```

Example Responses

Status code: 200

Normal response to the PUT operation. For more status codes, see [Status Codes](#).

```
{
  "firewall" : {
    "id" : "e9a7731d-5bd9-4250-a524-b9a076fd5629",
    "name" : "network_acl_test1",
    "description" : "network_acl_test1",
    "project_id" : "9476ea5a8a9849c38358e43c0c3a9e12",
    "created_at" : "2022-04-07T07:30:46.000+00:00",
    "updated_at" : "2022-04-07T07:30:46.000+00:00",
    "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"
} ],
"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"
} ],
"associations" : [ {
  "vsubnet_id" : "8359e5b0-353f-4ef3-a071-98e67a34a143"
} ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Change the name and description of the network ACL whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5629** to **network_acl_test1** and enable the network ACL.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class UpdateFirewallSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
```

```
.withProjectId(projectId)
.withAk(ak)
.withSk(sk);

VpcClient client = VpcClient.newBuilder()
    .withCredential(auth)
    .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
    .build();
UpdateFirewallRequest request = new UpdateFirewallRequest();
request.withFirewallId("{firewall_id}");
UpdateFirewallRequestBody body = new UpdateFirewallRequestBody();
UpdateFirewallOption firewallbody = new UpdateFirewallOption();
firewallbody.withName("network_acl_test1")
    .withDescription("network_acl_test1")
    .withAdminStateUp(true);
body.withFirewall(firewallbody);
request.withBody(body);
try {
    UpdateFirewallResponse response = client.updateFirewall(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

Change the name and description of the network ACL whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5629** to **network_acl_test1** and enable the network ACL.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.valueOf("<YOUR REGION>")) \
        .build()

    try:
        request = UpdateFirewallRequest()
        request.firewall_id = "{firewall_id}"
```

```
firewallbody = UpdateFirewallOption(  
    name="network_acl_test1",  
    description="network_acl_test1",  
    admin_state_up=True  
)  
request.body = UpdateFirewallRequestBody(  
    firewall=firewallbody  
)  
response = client.update_firewall(request)  
print(response)  
except exceptions.ClientRequestException as e:  
    print(e.status_code)  
    print(e.request_id)  
    print(e.error_code)  
    print(e.error_msg)
```

Go

Change the name and description of the network ACL whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5629** to **network_acl_test1** and enable the network ACL.

```
package main  
  
import (  
    "fmt"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"  
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"  
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"  
)  
  
func main() {  
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security  
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment  
    // variables and decrypted during use to ensure security.  
    // In this example, AK and SK are stored in environment variables for authentication. Before running this  
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment  
    ak := os.Getenv("CLOUD_SDK_AK")  
    sk := os.Getenv("CLOUD_SDK_SK")  
    projectId := "{project_id}"  
  
    auth := basic.NewCredentialsBuilder().  
        WithAk(ak).  
        WithSk(sk).  
        WithProjectId(projectId).  
        Build()  
  
    client := vpc.NewVpcClient(  
        vpc.VpcClientBuilder().  
            WithRegion(region.ValueOf("<YOUR REGION>")).  
            WithCredential(auth).  
            Build())  
  
    request := &model.UpdateFirewallRequest{  
        request.FirewallId = "{firewall_id}"  
        nameFirewall:= "network_acl_test1"  
        descriptionFirewall:= "network_acl_test1"  
        adminStateUpFirewall:= true  
        firewallbody := &model.UpdateFirewallOption{  
            Name: &nameFirewall,  
            Description: &descriptionFirewall,  
            AdminStateUp: &adminStateUpFirewall,  
        }  
        request.Body = &model.UpdateFirewallRequestBody{  
            Firewall: firewallbody,  
        }  
    }  
    response, err := client.UpdateFirewall(request)
```

```
if err == nil {  
    fmt.Printf("%+v\n", response)  
} else {  
    fmt.Println(err)  
}  
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Normal response to the PUT operation. For more 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.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v3/{project_id}/vpc/firewalls/{firewall_id}

Table 5-249 Path Parameters

Parameter	Mandatory	Type	Description
firewall_id	Yes	String	Unique ID of a network ACL.
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see Obtaining a Project ID .

Request Parameters

None

Response Parameters

Status code: 204

Normal response to the DELETE operation. For more status codes, see [Status Codes](#).

None

Example Requests

Deleting a network ACL

```
DELETE https://{Endpoint}/v3/{project_id}/vpc/firewalls/{firewall_id}
```

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class DeleteFirewallSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();

        DeleteFirewallRequest request = new DeleteFirewallRequest();
```

```
request.withFirewallId("{firewall_id}");
try {
    DeleteFirewallResponse response = client.deleteFirewall(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteFirewallRequest()
        request.firewall_id = "{firewall_id}"
        response = client.delete_firewall(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
```

```
// The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
// In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak := os.Getenv("CLOUD_SDK_AK")
sk := os.Getenv("CLOUD_SDK_SK")
projectId := "{project_id}"

auth := basic.NewCredentialsBuilder().
    WithAk(ak).
    WithSk(sk).
    WithProjectId(projectId).
    Build()

client := vpc.NewVpcClient(
    vpc.VpcClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.DeleteFirewallRequest{}
request.FirewallId = "{firewall_id}"
response, err := client.DeleteFirewall(request)
if err == nil {
    fmt.Printf("%v\n", response)
} else {
    fmt.Println(err)
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
204	Normal response to the DELETE operation. For more 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.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v3/{project_id}/vpc/firewalls/{firewall_id}/update-rules

Table 5-250 Path Parameters

Parameter	Mandatory	Type	Description
firewall_id	Yes	String	Unique ID of a network ACL.
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see Obtaining a Project ID .

Request Parameters

Table 5-251 Request body parameters

Parameter	Mandatory	Type	Description
firewall	Yes	FirewallUpdateRuleOption object	Inbound or outbound network ACL rules to be updated.

Table 5-252 FirewallUpdateRuleOption

Parameter	Mandatory	Type	Description
ingress_rules	No	Array of FirewallUpdateRuleItemOption objects	- Inbound network ACL rules to be updated. ingress_rules and egress_rules cannot be specified at the same time. Only one rule can be updated at a time.
egress_rules	No	Array of FirewallUpdateRuleItemOption objects	- Outbound network ACL rules to be updated. ingress_rules and egress_rules cannot be specified 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 (.).
description	No	String	- Description about the 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. allow indicates traffic is allowed and deny indicates that traffic is denied.
protocol	No	String	- Network ACL rule protocol. - The value can be tcp, udp, icmp, icmpv6, or an IP protocol number (0-255). 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 specified at the same time.

Parameter	Mandatory	Type	Description
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 specified 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 maximum number of port entries is 20 by default.
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 maximum number of port entries is 20 by default.
source_addresses_group_id	No	String	- Source IP address group ID of a network ACL rule. source_ip_address and source_address_group_id cannot be specified 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 specified at the same time.

Parameter	Mandatory	Type	Description
enabled	No	Boolean	- Whether to enable a network ACL rule. true means to enable the network ACL rule and false means to disable the network ACL rule. - The default value is 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	- The unique ID of 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	- Description about the network ACL. - The value can contain no more than 255 characters. - The value cannot contain angle brackets (< or >).
project_id	String	ID of the project that is associated with the network ACL.

Parameter	Type	Description
created_at	String	- Time when the network ACL was created. - The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ss</i>, which is automatically generated by the system.
updated_at	String	- Time when the network ACL was last updated. - The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ss</i>, which is automatically generated by the system.
admin_state_up	Boolean	- Whether a network ACL is enabled. - The value can be true (enabled) or false (disabled).
status	String	Network ACL status.
enterprise_project_id	String	- ID of the enterprise project that is associated with the network ACL. - The project ID can be 0 or a string that contains a maximum of 36 characters in UUID format with hyphens (-). 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 5-256 ResourceTag

Parameter	Type	Description
key	String	- Tag key - Tag keys must be unique for each resource. - The value can contain 1 to 128 characters. Minimum: 1 Maximum: 128
value	String	- Tag value. - The value can contain no more than 255 characters Maximum: 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 (.).
description	String	- Description about the 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. allow indicates traffic is allowed and deny indicates that traffic is denied.
project_id	String	ID of the project that is associated with a network ACL rule.
protocol	String	- Network ACL rule protocol. - The value can be tcp, udp, icmp, icmpv6, or an IP protocol number (0-255).
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 specified 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 specified 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 maximum number of port entries is 20 by default.
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 maximum number of port entries is 20 by default.

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 specified 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 specified at the same time.
enabled	Boolean	- Whether to enable a network ACL rule. true means to enable the network ACL rule and false means to disable the network ACL rule. - The default value is true.

Example Requests

Update the inbound rule whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5629** in the network ACL whose ID is **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 Responses

Status code: 200

Normal response to the PUT operation. For more status codes, see [Status Codes](#).

```
{
  "firewall" : {
    "id" : "e9a7731d-5bd9-4250-a524-b9a076fd5629",
```



```
{
  "name": "network_acl_test1",
  "description": "network_acl_test1",
  "project_id": "9476ea5a8a9849c38358e43c0c3a9e12",
  "created_at": "2022-04-07T07:30:46.000+00:00",
  "updated_at": "2022-04-07T07:30:46.000+00:00",
  "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"
  } ],
  "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"
  } ],
  "associations": [ {
    "vsubnet_id": "8359e5b0-353f-4ef3-a071-98e67a34a143"
  } ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Update the inbound rule whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5629** in the network ACL whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5629**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

import java.util.List;
import java.util.ArrayList;

public class UpdateFirewallRulesSolution {

    public static void main(String[] args) {
```

```
// The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
environment variables and decrypted during use to ensure security.
// In this example, AK and SK are stored in environment variables for authentication. Before running
this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
String ak = System.getenv("CLOUD_SDK_AK");
String sk = System.getenv("CLOUD_SDK_SK");
String projectId = "{project_id}";

ICredential auth = new BasicCredentials()
    .withProjectId(projectId)
    .withAk(ak)
    .withSk(sk);

VpcClient client = VpcClient.newBuilder()
    .withCredential(auth)
    .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
    .build();
UpdateFirewallRulesRequest request = new UpdateFirewallRulesRequest();
request.withFirewallId("{firewall_id}");
UpdateFirewallRulesRequestBody body = new UpdateFirewallRulesRequestBody();
List<FirewallUpdateRuleItemOption> listFirewallIngressRules = new ArrayList<>();
listFirewallIngressRules.add(
    new FirewallUpdateRuleItemOption()
        .withId("e9a7731d-5bd9-4250-a524-b9a076fd5629")
        .withName("network_acl_rule test2")
        .withDescription("network_acl_rule test2")
        .withAction("allow")
        .withProtocol("tcp")
        .withIpVersion(4)
        .withSourceIpAddress("192.168.3.0/24")
        .withDestinationIpAddress("192.168.6.0/24")
        .withSourcePort("30-40,60-90")
        .withDestinationPort("40-60,70-90")
);
FirewallUpdateRuleOption firewallbody = new FirewallUpdateRuleOption();
firewallbody.withIngressRules(listFirewallIngressRules);
body.withFirewall(firewallbody);
request.withBody(body);
try {
    UpdateFirewallRulesResponse response = client.updateFirewallRules(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

Update the inbound rule whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5629** in the network ACL whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5629**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *
```

```
if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdateFirewallRulesRequest()
        request.firewall_id = "{firewall_id}"
        listIngressRulesFirewall = [
            FirewallUpdateRuleItemOption(
                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"
            )
        ]
        firewallbody = FirewallUpdateRuleOption(
            ingress_rules=listIngressRulesFirewall
        )
        request.body = UpdateFirewallRulesRequestBody(
            firewall=firewallbody
        )
        response = client.update_firewall_rules(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Update the inbound rule whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5629** in the network ACL whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5629**.

package main

```
import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
```

```
ak := os.Getenv("CLOUD_SDK_AK")
sk := os.Getenv("CLOUD_SDK_SK")
projectId := "{project_id}"

auth := basic.NewCredentialsBuilder().
    WithAk(ak).
    WithSk(sk).
    WithProjectId(projectId).
    Build()

client := vpc.NewVpcClient(
    vpc.VpcClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.UpdateFirewallRulesRequest{}
request.FirewallId = "{firewall_id}"
nameIngressRules:= "network_acl_rule test2"
descriptionIngressRules:= "network_acl_rule test2"
actionIngressRules:= "allow"
protocolIngressRules:= "tcp"
ipVersionIngressRules:= int32(4)
sourceIpAddressIngressRules:= "192.168.3.0/24"
destinationIpAddressIngressRules:= "192.168.6.0/24"
sourcePortIngressRules:= "30-40,60-90"
destinationPortIngressRules:= "40-60,70-90"
var listIngressRulesFirewall = []model.FirewallUpdateRuleItemOption{
    {
        Id: "e9a7731d-5bd9-4250-a524-b9a076fd5629",
        Name: &nameIngressRules,
        Description: &descriptionIngressRules,
        Action: &actionIngressRules,
        Protocol: &protocolIngressRules,
        IpVersion: &ipVersionIngressRules,
        SourceIpAddress: &sourceIpAddressIngressRules,
        DestinationIpAddress: &destinationIpAddressIngressRules,
        SourcePort: &sourcePortIngressRules,
        DestinationPort: &destinationPortIngressRules,
    },
}
firewallbody := &model.FirewallUpdateRuleOption{
    IngressRules: &listIngressRulesFirewall,
}
request.Body = &model.UpdateFirewallRulesRequestBody{
    Firewall: firewallbody,
}
response, err := client.UpdateFirewallRules(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Normal response to the PUT operation. For more 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.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v3/{project_id}/vpc/firewalls/{firewall_id}/insert-rules

Table 5-259 Path Parameters

Parameter	Mandatory	Type	Description
firewall_id	Yes	String	Unique ID of a network ACL.
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see Obtaining a Project ID .

Request Parameters

Table 5-260 Request body parameters

Parameter	Mandatory	Type	Description
firewall	Yes	FirewallInsertRuleOption object	Details about the inbound and outbound network ACL rules to be inserted.

Table 5-261 FirewallInsertRuleOption

Parameter	Mandatory	Type	Description
ingress_rules	No	Array of FirewallInsertRuleItemOption objects	• Inbound network ACL rules to be inserted.
egress_rules	No	Array of FirewallInsertRuleItemOption objects	• Outbound network ACL rules to be inserted.
insert_after_rule	No	String	• Whether to insert a network ACL rule below an inbound or outbound rule. If insert_after_rule is not specified, the rule is inserted at the top of the inbound or outbound rule list. • If insert_after_rule is specified, ingress_rules and egress_rules cannot be specified at the same time, and the rule must be existing inbound or outbound rule.

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	• Description about the network ACL rule. • The value can contain no more than 255 characters. • The value cannot contain angle brackets (< or >).

Parameter	Mandatory	Type	Description
action	Yes	String	- Whether a network ACL rule allows or denies traffic. allow indicates traffic is allowed and deny indicates that traffic is denied.
protocol	Yes	String	- Network ACL rule protocol. - The value can be tcp, udp, icmp, icmpv6, or an IP protocol number (0–255). 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 specified 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 specified 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 maximum number of port entries is 20 by default.

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 maximum number of port entries is 20 by default.
source_addresses_group_id	No	String	- Source IP address group ID of a network ACL rule. source_ip_address and source_address_group_id cannot be specified at the same time.
destination_addresses_group_id	No	String	- Destination IP address group ID of a network ACL rule. destination_ip_address and destination_address_group_id cannot be specified at the same time.
enabled	No	Boolean	- Whether to enable a network ACL rule. true means to enable the network ACL rule and false means to disable the network ACL rule.- - - The default value is true.

Response Parameters

Status code: 200

Table 5-263 Response body parameters

Parameter	Type	Description
firewall	FirewallDetail object	Details after the network ACL rules are inserted.
request_id	String	Request ID.

Table 5-264 FirewallDetail

Parameter	Type	Description
id	String	- The unique ID of 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	- Description about the network ACL. - The value can contain no more than 255 characters. - The value cannot contain angle brackets (< or >).
project_id	String	ID of the project that is associated with the network ACL.
created_at	String	- Time when the network ACL was created. - The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ss</i>, which is automatically generated by the system.
updated_at	String	- Time when the network ACL was last updated. - The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ss</i>, which is automatically generated by the system.
admin_state_up	Boolean	- Whether a network ACL is enabled. - The value can be true (enabled) or false (disabled).
status	String	Network ACL status.
enterprise_project_id	String	- ID of the enterprise project that is associated with the network ACL. - The project ID can be 0 or a string that contains a maximum of 36 characters in UUID format with hyphens (-). 0 indicates the default enterprise project.

Parameter	Type	Description
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 5-265 ResourceTag

Parameter	Type	Description
key	String	- Tag key - Tag keys must be unique for each resource. - The value can contain 1 to 128 characters. Minimum: 1 Maximum: 128
value	String	- Tag value. - The value can contain no more than 255 characters Maximum: 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 (.).
description	String	- Description about the 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. allow indicates traffic is allowed and deny indicates that traffic is denied.
project_id	String	ID of the project that is associated with a network ACL rule.
protocol	String	- Network ACL rule protocol. - The value can be tcp, udp, icmp, icmpv6, or an IP protocol number (0-255).
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 specified 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 specified at the same time.

Parameter	Type	Description
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 maximum number of port entries is 20 by default.
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 maximum number of port entries is 20 by default.
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 specified 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 specified at the same time.
enabled	Boolean	- Whether to enable a network ACL rule. true means to enable the network ACL rule and false means to disable the network ACL rule. - The default value is true.

Example Requests

- Insert an inbound rule below the rule whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5630** to the network ACL whose ID is **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 test",
      "description": "network_acl_rule 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
}],
"insert_after_rule" : "e9a7731d-5bd9-4250-a524-b9a076fd5630"
}
}
```

- Insert an outbound rule below the rule whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5630** to the network ACL whose ID is **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 test",
      "description" : "network_acl_rule 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
    } ],
    "insert_after_rule" : "e9a7731d-5bd9-4250-a524-b9a076fd5630"
  }
}
```

Example Responses

Status code: 200

Normal response to the PUT operation. For more status codes, see [Status Codes](#).

```
{
  "firewall" : {
    "id" : "e9a7731d-5bd9-4250-a524-b9a076fd5629",
    "name" : "network_acl_test1",
    "description" : "network_acl_test1",
    "project_id" : "9476ea5a8a9849c38358e43c0c3a9e12",
    "created_at" : "2022-04-07T07:30:46.000+00:00",
    "updated_at" : "2022-04-07T07:30:46.000+00:00",
    "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"
    } ],
    "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"
}],
"associations" : [ {
  "vsubnet_id" : "8359e5b0-353f-4ef3-a071-98e67a34a143"
} ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

- Insert an inbound rule below the rule whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5630** to the network ACL whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5629**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

import java.util.List;
import java.util.ArrayList;

public class AddFirewallRulesSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before
        // running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local
        // environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR_REGION>"))
            .build();
        AddFirewallRulesRequest request = new AddFirewallRulesRequest();
        request.withFirewallId("{firewall_id}");
        AddFirewallRulesRequestBody body = new AddFirewallRulesRequestBody();
        List<FirewallInsertRuleItemOption> listFirewallIngressRules = new ArrayList<>();
```

```
listFirewallIngressRules.add(
    new FirewallInsertRuleItemOption()
        .withName("network_acl_rule test")
        .withDescription("network_acl_rule test")
        .withAction("allow")
        .withProtocol("tcp")
        .withIpVersion(4)
        .withSourceIpAddress("192.168.3.0/24")
        .withDestinationIpAddress("192.168.6.0/24")
        .withSourcePort("30-40,60-90")
        .withDestinationPort("40-60,70-90")
);
FirewallInsertRuleOption firewallbody = new FirewallInsertRuleOption();
firewallbody.withIngressRules(listFirewallIngressRules)
    .withInsertAfterRule("e9a7731d-5bd9-4250-a524-b9a076fd5630");
body.withFirewall(firewallbody);
request.withBody(body);
try {
    AddFirewallRulesResponse response = client.addFirewallRules(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

- Insert an outbound rule below the rule whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5630** to the network ACL whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5629**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

import java.util.List;
import java.util.ArrayList;

public class AddFirewallRulesSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before
        // running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local
        // environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);
```

```
VpcClient client = VpcClient.newBuilder()
    .withCredential(auth)
    .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
    .build();
AddFirewallRulesRequest request = new AddFirewallRulesRequest();
request.withFirewallId("{firewall_id}");
AddFirewallRulesRequestBody body = new AddFirewallRulesRequestBody();
List<FirewallInsertRuleItemOption> listFirewallEgressRules = new ArrayList<>();
listFirewallEgressRules.add(
    new FirewallInsertRuleItemOption()
        .withName("network_acl_rule test")
        .withDescription("network_acl_rule test")
        .withAction("allow")
        .withProtocol("tcp")
        .withIpVersion(4)
        .withSourceIpAddress("192.168.3.0/24")
        .withDestinationIpAddress("192.168.6.0/24")
        .withSourcePort("30-40,60-90")
        .withDestinationPort("40-60,70-90")
);
FirewallInsertRuleOption firewallbody = new FirewallInsertRuleOption();
firewallbody.withEgressRules(listFirewallEgressRules)
    .withInsertAfterRule("e9a7731d-5bd9-4250-a524-b9a076fd5630");
body.withFirewall(firewallbody);
request.withBody(body);
try {
    AddFirewallRulesResponse response = client.addFirewallRules(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

- Insert an inbound rule below the rule whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5630** to the network ACL whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5629**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
    # security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
    # environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before
    # running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local
    # environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)
```



```
client = VpcClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(VpcRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = AddFirewallRulesRequest()
    request.firewall_id = "{firewall_id}"
    listIngressRulesFirewall = [
        FirewallInsertRuleItemOption(
            name="network_acl_rule test",
            description="network_acl_rule 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"
        )
    ]
    firewallbody = FirewallInsertRuleOption(
        ingress_rules=listIngressRulesFirewall,
        insert_after_rule="e9a7731d-5bd9-4250-a524-b9a076fd5630"
    )
    request.body = AddFirewallRulesRequestBody(
        firewall=firewallbody
    )
    response = client.add_firewall_rules(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

- Insert an outbound rule below the rule whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5630** to the network ACL whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5629**.

coding: utf-8

```
import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
    # security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
    # environment variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before
    # running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local
    # environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = AddFirewallRulesRequest()
        request.firewall_id = "{firewall_id}"
        listEgressRulesFirewall = [
```

```
        FirewallInsertRuleItemOption(  
            name="network_acl_rule test",  
            description="network_acl_rule 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"  
        )  
    ]  
    firewallbody = FirewallInsertRuleOption(  
        egress_rules=listEgressRulesFirewall,  
        insert_after_rule="e9a7731d-5bd9-4250-a524-b9a076fd5630"  
    )  
    request.body = AddFirewallRulesRequestBody(  
        firewall=firewallbody  
    )  
    response = client.add_firewall_rules(request)  
    print(response)  
except exceptions.ClientRequestException as e:  
    print(e.status_code)  
    print(e.request_id)  
    print(e.error_code)  
    print(e.error_msg)
```

Go

- Insert an inbound rule below the rule whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5630** to the network ACL whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5629**.

```
package main  
  
import (  
    "fmt"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"  
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"  
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"  
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"  
)  
  
func main() {  
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great  
    // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or  
    // environment variables and decrypted during use to ensure security.  
    // In this example, AK and SK are stored in environment variables for authentication. Before  
    // running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local  
    // environment  
    ak := os.Getenv("CLOUD_SDK_AK")  
    sk := os.Getenv("CLOUD_SDK_SK")  
    projectId := "{project_id}"  
  
    auth := basic.NewCredentialsBuilder().  
        WithAk(ak).  
        WithSk(sk).  
        WithProjectId(projectId).  
        Build()  
  
    client := vpc.NewVpcClient(  
        vpc.VpcClientBuilder().  
            WithRegion(region.ValueOf("<YOUR REGION>")).  
            WithCredential(auth).  
            Build()  
    )  
  
    request := &model.AddFirewallRulesRequest{  
        request.FirewallId = "{firewall_id}"  
        nameIngressRules:= "network_acl_rule test"  
    }
```

```
descriptionIngressRules:= "network_acl_rule test"
sourceIpAddressIngressRules:= "192.168.3.0/24"
destinationIpAddressIngressRules:= "192.168.6.0/24"
sourcePortIngressRules:= "30-40,60-90"
destinationPortIngressRules:= "40-60,70-90"
var listIngressRulesFirewall = []model.FirewallInsertRuleItemOption{
    {
        Name: &nameIngressRules,
        Description: &descriptionIngressRules,
        Action: "allow",
        Protocol: "tcp",
        IpVersion: int32(4),
        SourceIpAddress: &sourceIpAddressIngressRules,
        DestinationIpAddress: &destinationIpAddressIngressRules,
        SourcePort: &sourcePortIngressRules,
        DestinationPort: &destinationPortIngressRules,
    },
}
insertAfterRuleFirewall:= "e9a7731d-5bd9-4250-a524-b9a076fd5630"
firewallbody := &model.FirewallInsertRuleOption{
    IngressRules: &listIngressRulesFirewall,
    InsertAfterRule: &insertAfterRuleFirewall,
}
request.Body = &model.AddFirewallRulesRequestBody{
    Firewall: firewallbody,
}
response, err := client.AddFirewallRules(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}
```

- Insert an outbound rule below the rule whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5630** to the network ACL whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5629**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
    // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
    // environment variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before
    // running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local
    // environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())
```

```
request := &model.AddFirewallRulesRequest{}
request.FirewallId = "{firewall_id}"
nameEgressRules:= "network_acl_rule test"
descriptionEgressRules:= "network_acl_rule test"
sourceIpAddressEgressRules:= "192.168.3.0/24"
destinationIpAddressEgressRules:= "192.168.6.0/24"
sourcePortEgressRules:= "30-40,60-90"
destinationPortEgressRules:= "40-60,70-90"
var listEgressRulesFirewall = []model.FirewallInsertRuleItemOption{
    {
        Name: &nameEgressRules,
        Description: &descriptionEgressRules,
        Action: "allow",
        Protocol: "tcp",
        IpVersion: int32(4),
        SourceIpAddress: &sourceIpAddressEgressRules,
        DestinationIpAddress: &destinationIpAddressEgressRules,
        SourcePort: &sourcePortEgressRules,
        DestinationPort: &destinationPortEgressRules,
    },
}
insertAfterRuleFirewall:= "e9a7731d-5bd9-4250-a524-b9a076fd5630"
firewallbody := &model.FirewallInsertRuleOption{
    EgressRules: &listEgressRulesFirewall,
    InsertAfterRule: &insertAfterRuleFirewall,
}
request.Body = &model.AddFirewallRulesRequestBody{
    Firewall: firewallbody,
}
response, err := client.AddFirewallRules(request)
if err == nil {
    fmt.Printf("%v\n", response)
} else {
    fmt.Println(err)
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Normal response to the PUT operation. For more 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.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v3/{project_id}/vpc/firewalls/{firewall_id}/remove-rules

Table 5-268 Path Parameters

Parameter	Mandatory	Type	Description
firewall_id	Yes	String	Unique ID of a network ACL.
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see Obtaining a Project ID .

Request Parameters

Table 5-269 Request body parameters

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	- Inbound network ACL rules to be deleted. ingress_rules and egress_rules cannot be specified at the same time.
egress_rules	No	Array of FirewallRemoveRuleItemOption objects	- Outbound network ACL rules to be deleted. ingress_rules and egress_rules cannot be specified 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	- The unique ID of 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	- Description about the network ACL. - The value can contain no more than 255 characters. - The value cannot contain angle brackets (< or >).
project_id	String	ID of the project that is associated with the network ACL.
created_at	String	- Time when the network ACL was created. - The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ss</i>, which is automatically generated by the system.

Parameter	Type	Description
updated_at	String	- Time when the network ACL was last updated. - The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ss</i>, which is automatically generated by the system.
admin_state_up	Boolean	- Whether a network ACL is enabled. - The value can be true (enabled) or false (disabled).
status	String	Network ACL status.
enterprise_project_id	String	- ID of the enterprise project that is associated with the network ACL. - The project ID can be 0 or a string that contains a maximum of 36 characters in UUID format with hyphens (-). 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 5-274 ResourceTag

Parameter	Type	Description
key	String	- Tag key - Tag keys must be unique for each resource. - The value can contain 1 to 128 characters. Minimum: 1 Maximum: 128

Parameter	Type	Description
value	String	- Tag value. - The value can contain no more than 255 characters Maximum: 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	- Description about the 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. allow indicates traffic is allowed and deny indicates that traffic is denied.
project_id	String	ID of the project that is associated with a network ACL rule.

Parameter	Type	Description
protocol	String	- Network ACL rule protocol. - The value can be tcp, udp, icmp, icmpv6, or an IP protocol number (0–255).
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 specified 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 specified 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 maximum number of port entries is 20 by default.
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 maximum number of port entries is 20 by default.
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 specified 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 specified at the same time.

Parameter	Type	Description
enabled	Boolean	- Whether to enable a network ACL rule. true means to enable the network ACL rule and false means to disable the network ACL rule. - The default value is true.

Example Requests

Delete the inbound rule whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5629** from the network ACL whose ID is **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 Responses

Status code: 200

Normal response to the PUT operation. For more status codes, see [Status Codes](#).

```
{
  "firewall": {
    "id": "e9a7731d-5bd9-4250-a524-b9a076fd5629",
    "name": "network_acl_test1",
    "description": "network_acl_test1",
    "project_id": "9476ea5a8a9849c38358e43c0c3a9e12",
    "created_at": "2022-04-07T07:30:46.000+00:00",
    "updated_at": "2022-04-07T07:30:46.000+00:00",
    "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"
    } ],
    "associations": [ {
      "vsubnet_id": "8359e5b0-353f-4ef3-a071-98e67a34a143"
    } ]
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Delete the inbound rule whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5629** from the network ACL whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5629**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

import java.util.List;
import java.util.ArrayList;

public class RemoveFirewallRulesSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();

        RemoveFirewallRulesRequest request = new RemoveFirewallRulesRequest();
        request.withFirewallId("{firewall_id}");
        RemoveFirewallRulesRequestBody body = new RemoveFirewallRulesRequestBody();
        List<FirewallRemoveRuleItemOption> listFirewallIngressRules = new ArrayList<>();
        listFirewallIngressRules.add(
            new FirewallRemoveRuleItemOption()
                .withId("e9a7731d-5bd9-4250-a524-b9a076fd5629")
        );
        FirewallRemoveRuleOption firewallbody = new FirewallRemoveRuleOption();
        firewallbody.withIngressRules(listFirewallIngressRules);
        body.withFirewall(firewallbody);
        request.withBody(body);
        try {
            RemoveFirewallRulesResponse response = client.removeFirewallRules(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
        }
    }
}
```

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

Python

Delete the inbound rule whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5629** from the network ACL whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5629**.

coding: utf-8

```
import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = RemoveFirewallRulesRequest()
        request.firewall_id = "{firewall_id}"
        listIngressRulesFirewall = [
            FirewallRemoveRuleItemOption(
                id="e9a7731d-5bd9-4250-a524-b9a076fd5629"
            )
        ]
        firewallbody = FirewallRemoveRuleOption(
            ingress_rules=listIngressRulesFirewall
        )
        request.body = RemoveFirewallRulesRequestBody(
            firewall=firewallbody
        )
        response = client.remove_firewall_rules(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Delete the inbound rule whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5629** from the network ACL whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5629**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
```

```
vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
"github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.RemoveFirewallRulesRequest{}
    request.FirewallId = "{firewall_id}"
    var listIngressRulesFirewall = []model.FirewallRemoveRuleItemOption{
        {
            Id: "e9a7731d-5bd9-4250-a524-b9a076fd5629",
        },
    }
    firewallbody := &model.FirewallRemoveRuleOption{
        IngressRules: &listIngressRulesFirewall,
    }
    request.Body = &model.RemoveFirewallRulesRequestBody{
        Firewall: firewallbody,
    }
    response, err := client.RemoveFirewallRules(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Normal response to the PUT operation. For more 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.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v3/{project_id}/vpc/firewalls/{firewall_id}/associate-subnets

Table 5-277 Path Parameters

Parameter	Mandatory	Type	Description
firewall_id	Yes	String	Unique ID of a network ACL.
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see Obtaining a Project ID .

Request Parameters

Table 5-278 Request body parameters

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	IDs of subnets that are 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	- The unique ID of 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	- Description about the network ACL. - The value can contain no more than 255 characters. - The value cannot contain angle brackets (< or >).
project_id	String	ID of the project that is associated with the network ACL.
created_at	String	- Time when the network ACL was created. - The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ss</i>, which is automatically generated by the system.
updated_at	String	- Time when the network ACL was last updated. - The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ss</i>, which is automatically generated by the system.

Parameter	Type	Description
admin_state_up	Boolean	- Whether a network ACL is enabled. - The value can be true (enabled) or false (disabled).
status	String	Network ACL status.
enterprise_project_id	String	- ID of the enterprise project that is associated with the network ACL. - The project ID can be 0 or a string that contains a maximum of 36 characters in UUID format with hyphens (-). 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. - The value can contain 1 to 128 characters. Minimum: 1 Maximum: 128
value	String	- Tag value. - The value can contain no more than 255 characters Maximum: 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	- Description about the 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. allow indicates traffic is allowed and deny indicates that traffic is denied.
project_id	String	ID of the project that is associated with a network ACL rule.
protocol	String	- Network ACL rule protocol. - The value can be tcp, udp, icmp, icmpv6, or an IP protocol number (0-255).
ip_version	Integer	- IP version of a network ACL rule. - The value can be 4 (IPv4) or 6 (IPv6).

Parameter	Type	Description
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 specified 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 specified 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 maximum number of port entries is 20 by default.
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 maximum number of port entries is 20 by default.
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 specified 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 specified at the same time.
enabled	Boolean	- Whether to enable a network ACL rule. true means to enable the network ACL rule and false means to disable the network ACL rule. - The default value is true.

Example Requests

Associate the subnet whose ID is **8359e5b0-353f-4ef3-a071-98e67a34a143** with the network ACL whose ID is **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 Responses

Status code: 200

Normal response to the PUT operation. For more status codes, see [Status Codes](#).

```
{
  "firewall": {
    "id": "e9a7731d-5bd9-4250-a524-b9a076fd5629",
    "name": "network_acl_test1",
    "description": "network_acl_test1",
    "project_id": "9476ea5a8a9849c38358e43c0c3a9e12",
    "created_at": "2022-04-07T07:30:46.000+00:00",
    "updated_at": "2022-04-07T07:30:46.000+00:00",
    "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"
    } ],
    "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"
    } ],
    "associations": [ {
      "virsubnet_id": "8359e5b0-353f-4ef3-a071-98e67a34a143"
    } ]
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Associate the subnet whose ID is **8359e5b0-353f-4ef3-a071-98e67a34a143** with the network ACL whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5629**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

import java.util.List;
import java.util.ArrayList;

public class AssociateSubnetFirewallSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();
        AssociateSubnetFirewallRequest request = new AssociateSubnetFirewallRequest();
        request.withFirewallId("{firewall_id}");
        AssociateSubnetFirewallRequestBody body = new AssociateSubnetFirewallRequestBody();
        List<FirewallAssociation> listbodySubnets = new ArrayList<>();
        listbodySubnets.add(
            new FirewallAssociation()
                .withVirsubnetId("8359e5b0-353f-4ef3-a071-98e67a34a143")
        );
        body.withSubnets(listbodySubnets);
        request.withBody(body);
        try {
            AssociateSubnetFirewallResponse response = client.associateSubnetFirewall(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Associate the subnet whose ID is **8359e5b0-353f-4ef3-a071-98e67a34a143** with the network ACL whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5629**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = AssociateSubnetFirewallRequest()
        request.firewall_id = "{firewall_id}"
        listSubnetsbody = [
            FirewallAssociation(
                vsubnet_id="8359e5b0-353f-4ef3-a071-98e67a34a143"
            )
        ]
        request.body = AssociateSubnetFirewallRequestBody(
            subnets=listSubnetsbody
        )
        response = client.associate_subnet_firewall(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Associate the subnet whose ID is **8359e5b0-353f-4ef3-a071-98e67a34a143** with the network ACL whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5629**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
```

```
// In this example, AK and SK are stored in environment variables for authentication. Before running this
example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak := os.Getenv("CLOUD_SDK_AK")
sk := os.Getenv("CLOUD_SDK_SK")
projectId := "{project_id}"

auth := basic.NewCredentialsBuilder().
    WithAk(ak).
    WithSk(sk).
    WithProjectId(projectId).
    Build()

client := vpc.NewVpcClient(
    vpc.VpcClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.AssociateSubnetFirewallRequest{}
request.FirewallId = "{firewall_id}"
var listSubnetsbody = []model.FirewallAssociation{
    {
        VirsubnetId: "8359e5b0-353f-4ef3-a071-98e67a34a143",
    },
}
request.Body = &model.AssociateSubnetFirewallRequestBody{
    Subnets: listSubnetsbody,
}
response, err := client.AssociateSubnetFirewall(request)
if err == nil {
    fmt.Printf("%v\n", response)
} else {
    fmt.Println(err)
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Normal response to the PUT operation. For more 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.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v3/{project_id}/vpc/firewalls/{firewall_id}/disassociate-subnets

Table 5-285 Path Parameters

Parameter	Mandatory	Type	Description
firewall_id	Yes	String	Unique ID of a network ACL.
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see Obtaining a Project ID .

Request Parameters

Table 5-286 Request body parameters

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	IDs of subnets that are 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.

Parameter	Type	Description
request_id	String	Request ID.

Table 5-289 FirewallDetail

Parameter	Type	Description
id	String	- The unique ID of 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	- Description about the network ACL. - The value can contain no more than 255 characters. - The value cannot contain angle brackets (< or >).
project_id	String	ID of the project that is associated with the network ACL.
created_at	String	- Time when the network ACL was created. - The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ss</i>, which is automatically generated by the system.
updated_at	String	- Time when the network ACL was last updated. - The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ss</i>, which is automatically generated by the system.
admin_state_up	Boolean	- Whether a network ACL is enabled. - The value can be true (enabled) or false (disabled).
status	String	Network ACL status.

Parameter	Type	Description
enterprise_project_id	String	- ID of the enterprise project that is associated with the network ACL. - The project ID can be 0 or a string that contains a maximum of 36 characters in UUID format with hyphens (-). 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 5-290 ResourceTag

Parameter	Type	Description
key	String	- Tag key - Tag keys must be unique for each resource. - The value can contain 1 to 128 characters. Minimum: 1 Maximum: 128
value	String	- Tag value. - The value can contain no more than 255 characters Maximum: 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 (.).
description	String	- Description about the 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. allow indicates traffic is allowed and deny indicates that traffic is denied.
project_id	String	ID of the project that is associated with a network ACL rule.
protocol	String	- Network ACL rule protocol. - The value can be tcp, udp, icmp, icmpv6, or an IP protocol number (0-255).
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 specified at the same time.

Parameter	Type	Description
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 specified 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 maximum number of port entries is 20 by default.
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 maximum number of port entries is 20 by default.
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 specified 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 specified at the same time.
enabled	Boolean	- Whether to enable a network ACL rule. true means to enable the network ACL rule and false means to disable the network ACL rule. - The default value is true.

Example Requests

Disassociate subnets whose IDs are **8359e5b0-353f-4ef3-a071-98e67a34a143** and **d9994dcf-ef6d-47ec-9ac9-a62d4fd5e163** from the network ACL whose ID is **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 Responses

Status code: 200

Normal response to the PUT operation. For more status codes, see [Status Codes](#).

```
{
  "firewall": {
    "id": "e9a7731d-5bd9-4250-a524-b9a076fd5629",
    "name": "network_acl_test1",
    "description": "network_acl_test1",
    "project_id": "9476ea5a8a9849c38358e43c0c3a9e12",
    "created_at": "2022-04-07T07:30:46.000+00:00",
    "updated_at": "2022-04-07T07:30:46.000+00:00",
    "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"
    } ],
    "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"
    } ],
    "associations": [ ]
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Disassociate subnets whose IDs are **8359e5b0-353f-4ef3-a071-98e67a34a143** and **d9994dcf-ef6d-47ec-9ac9-a62d4fd5e163** from the network ACL whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5629**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

import java.util.List;
import java.util.ArrayList;

public class DisassociateSubnetFirewallSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();
        DisassociateSubnetFirewallRequest request = new DisassociateSubnetFirewallRequest();
        request.withFirewallId("{firewall_id}");
        DisassociateSubnetFirewallRequestBody body = new DisassociateSubnetFirewallRequestBody();
        List<FirewallAssociation> listbodySubnets = new ArrayList<>();
        listbodySubnets.add(
            new FirewallAssociation()
                .withVirsubnetId("8359e5b0-353f-4ef3-a071-98e67a34a143")
        );
        listbodySubnets.add(
            new FirewallAssociation()
                .withVirsubnetId("d9994dcf-ef6d-47ec-9ac9-a62d4fd5e163")
        );
        body.withSubnets(listbodySubnets);
        request.withBody(body);
        try {
            DisassociateSubnetFirewallResponse response = client.disassociateSubnetFirewall(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Disassociate subnets whose IDs are **8359e5b0-353f-4ef3-a071-98e67a34a143** and **d9994dcf-ef6d-47ec-9ac9-a62d4fd5e163** from the network ACL whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5629**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DisassociateSubnetFirewallRequest()
        request.firewall_id = "{firewall_id}"
        listSubnetsbody = [
            FirewallAssociation(
                virsubnet_id="8359e5b0-353f-4ef3-a071-98e67a34a143"
            ),
            FirewallAssociation(
                virsubnet_id="d9994dcf-ef6d-47ec-9ac9-a62d4fd5e163"
            )
        ]
        request.body = DisassociateSubnetFirewallRequestBody(
            subnets=listSubnetsbody
        )
        response = client.disassociate_subnet_firewall(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Disassociate subnets whose IDs are **8359e5b0-353f-4ef3-a071-98e67a34a143** and **d9994dcf-ef6d-47ec-9ac9-a62d4fd5e163** from the network ACL whose ID is **e9a7731d-5bd9-4250-a524-b9a076fd5629**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
```

```
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DisassociateSubnetFirewallRequest{}
    request.FirewallId = "{firewall_id}"
    var listSubnetsbody = []model.FirewallAssociation{
        {
            VirsubnetId: "8359e5b0-353f-4ef3-a071-98e67a34a143",
        },
        {
            VirsubnetId: "d9994dcf-ef6d-47ec-9ac9-a62d4fd5e163",
        },
    }
    request.Body = &model.DisassociateSubnetFirewallRequestBody{
        Subnets: listSubnetsbody,
    }
    response, err := client.DisassociateSubnetFirewall(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Normal response to the PUT operation. For more 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.

Calling Method

For details, see [Calling APIs](#).

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 .

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 5-295 Match

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. Currently, the tag key can only be the resource name. Minimum: 1 Maximum: 128
value	Yes	String	Tag value. Each value can contain a maximum of 255 Unicode characters. Minimum: 0 Maximum: 255

Table 5-296 ListTag

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. The key cannot be left blank. Minimum: 1 Maximum: 128

Parameter	Mandatory	Type	Description
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: 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

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. For more status codes, see [Status Codes](#).

```
{
  "request_id": "239df34e-a651-4631-aaa1-d5fef231933a",
  "total_count": 2
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Query network ACLs using tags and matches.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

import java.util.List;
import java.util.ArrayList;

public class CountFirewallsByTagsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();
        CountFirewallsByTagsRequest request = new CountFirewallsByTagsRequest();
        CountFirewallsByTagsRequestBody body = new CountFirewallsByTagsRequestBody();
        List<String> listTagsValues = new ArrayList<>();
        listTagsValues.add("value1");
        List<ListTag> listbodyTags = new ArrayList<>();
        listbodyTags.add(
            new ListTag()
                .withKey("key1")
                .withValues(listTagsValues)
        );
        List<Match> listbodyMatches = new ArrayList<>();
        listbodyMatches.add(
            new Match()
                .withKey("resource_name")
                .withValue("network_aclv3_test")
        );
        body.withTags(listbodyTags);
        body.withMatches(listbodyMatches);
        request.withBody(body);
        try {
            CountFirewallsByTagsResponse response = client.countFirewallsByTags(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
        }
    }
}
```

```
        System.out.println(e.getErrorCode());
        System.out.println(e.getErrorMsg());
    }
}
```

Python

Query network ACLs using tags and matches.

coding: utf-8

```
import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CountFirewallsByTagsRequest()
        listValuesTags = [
            "value1"
        ]
        listTagsbody = [
            ListTag(
                key="key1",
                values=listValuesTags
            )
        ]
        listMatchesbody = [
            Match(
                key="resource_name",
                value="network_aclv3_test"
            )
        ]
        request.body = CountFirewallsByTagsRequestBody(
            tags=listTagsbody,
            matches=listMatchesbody
        )
        response = client.count_firewalls_by_tags(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

Query network ACLs using tags and matches.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CountFirewallsByTagsRequest{}
    var listValuesTags = []string{
        "value1",
    }
    var listTagsbody = []model.ListTag{
        {
            Key: "key1",
            Values: listValuesTags,
        },
    }
    var listMatchesbody = []model.Match{
        {
            Key: "resource_name",
            Value: "network_aclv3_test",
        },
    }
    request.Body = &model.CountFirewallsByTagsRequestBody{
        Tags: &listTagsbody,
        Matches: &listMatchesbody,
    }
    response, err := client.CountFirewallsByTags(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Normal request response. For more status codes, see Status Codes .

Error Codes

See [Error Codes](#).

5.10.2 Querying Network ACLs Using Tags

Function

This API is used to query network ACLs using tags.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v3/{project_id}/firewalls/resource-instances/filter

Table 5-298 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 5-299 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

Parameter	Mandatory	Type	Description
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 5-300 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 5-301 Match

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. Currently, the tag key can only be the resource name. Minimum: 1 Maximum: 128
value	Yes	String	Tag value. Each value can contain a maximum of 255 Unicode characters. Minimum: 0 Maximum: 255

Table 5-302 ListTag

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. The key cannot be left blank. 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: 255

Response Parameters

Status code: 200

Table 5-303 Response body parameters

Parameter	Type	Description
resources	Array of ListResourceResp objects	Resources
total_count	Integer	Resource quantity
request_id	String	Request ID

Table 5-304 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 5-305 ResourceTag

Parameter	Type	Description
key	String	- Tag key - Tag keys must be unique for each resource. - The value can contain 1 to 128 characters. Minimum: 1 Maximum: 128
value	String	- Tag value. - The value can contain no more than 255 characters Maximum: 255

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. For more status codes, see [Status Codes](#).

```
{
  "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
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Query network ACLs using tags and matches. A maximum of 100 records can be returned. The query starts from the first record.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

import java.util.List;
import java.util.ArrayList;

public class ListFirewallsByTagsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
```

```
String sk = System.getenv("CLOUD_SDK_SK");
String projectId = "{project_id}";

ICredential auth = new BasicCredentials()
    .withProjectId(projectId)
    .withAk(ak)
    .withSk(sk);

VpcClient client = VpcClient.newBuilder()
    .withCredential(auth)
    .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
    .build();
ListFirewallsByTagsRequest request = new ListFirewallsByTagsRequest();
ListFirewallsByTagsRequestBody body = new ListFirewallsByTagsRequestBody();
[]string listTagsValues = new ArrayList<>();
listTagsValues.add("value1");
[](model.ListTag) listbodyTags = new ArrayList<>();
listbodyTags.add(
    new ListTag()
        .withKey("key1")
        .withValues(listTagsValues)
);
[](model.Match) listbodyMatches = new ArrayList<>();
listbodyMatches.add(
    new Match()
        .withKey("resource_name")
        .withValue("network_aclv3_test")
);
body.withTags(listbodyTags);
body.withMatches(listbodyMatches);
request.withBody(body);
try {
    ListFirewallsByTagsResponse response = client.listFirewallsByTags(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

Query network ACLs using tags and matches. A maximum of 100 records can be returned. The query starts from the first record.

coding: utf-8

```
import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *
```

```
if __name__ == "__main__":
```

```
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
```

```
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
```

```
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
```

```
projectId = "{project_id}"

credentials = BasicCredentials(ak, sk, projectId)

client = VpcClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(VpcRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = ListFirewallsByTagsRequest()
    listValuesTags = [
        "value1"
    ]
    listTagsbody = [
        ListTag(
            key="key1",
            values=listValuesTags
        )
    ]
    listMatchesbody = [
        Match(
            key="resource_name",
            value="network_aclv3_test"
        )
    ]
    request.body = ListFirewallsByTagsRequestBody(
        tags=listTagsbody,
        matches=listMatchesbody
    )
    response = client.list_firewalls_by_tags(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

Query network ACLs using tags and matches. A maximum of 100 records can be returned. The query starts from the first record.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewClient(
        region,
        auth,
    )

    request := model.ListFirewallsByTagsRequest()
    request.Tags = []string{"value1"}
    request.Matches = []string{"resource_name"}
    request.Value = "network_aclv3_test"

    response, err := client.ListFirewallsByTags(request)
    if err != nil {
        fmt.Println("Error: ", err)
    }
    fmt.Println(response)
```

```
client := vpc.NewVpcClient(  
    vpc.VpcClientBuilder().  
        WithRegion(region.ValueOf("<YOUR REGION>")).  
        WithCredential(auth).  
        Build())  
  
request := &model.ListFirewallsByTagsRequest{  
    var listValuesTags = []string{  
        "value1",  
    }  
    var listTagsbody = []model.ListTag{  
        {  
            Key: "key1",  
            Values: listValuesTags,  
        },  
    }  
    var listMatchesbody = []model.Match{  
        {  
            Key: "resource_name",  
            Value: "network_aclv3_test",  
        },  
    }  
    }  
request.Body = &model.ListFirewallsByTagsRequestBody{  
    Tags: &listTagsbody,  
    Matches: &listMatchesbody,  
}  
response, err := client.ListFirewallsByTags(request)  
if err == nil {  
    fmt.Printf("%+v\n", response)  
} else {  
    fmt.Println(err)  
}  
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Normal request response. For more status codes, see Status Codes .

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.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v3/{project_id}/firewalls/{firewall_id}/tags

Table 5-306 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 5-307 Request body parameters

Parameter	Mandatory	Type	Description
tag	Yes	ResourceTag object	Request body for adding tags to a network ACL.

Table 5-308 ResourceTag

Parameter	Mandatory	Type	Description
key	Yes	String	- Tag key - Tag keys must be unique for each resource. - The value can contain 1 to 128 characters. Minimum: 1 Maximum: 128
value	Yes	String	- Tag value. - The value can contain no more than 255 characters Maximum: 255

Response Parameters

Status code: 204

Normal request response. For more status codes, see [Status Codes](#).

None

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

SDK Sample Code

The SDK sample code is as follows.

Java

Add a tag to a network ACL. Set the tag key to **key4** and tag value to **value4**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class CreateFirewallTagSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
```

```
        .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
        .build();
CreateFirewallTagRequest request = new CreateFirewallTagRequest();
request.withFirewallId("{firewall_id}");
CreateFirewallTagRequestBody body = new CreateFirewallTagRequestBody();
ResourceTag tagbody = new ResourceTag();
tagbody.withKey("key4")
        .withValue("value4");
body.withTag(tagbody);
request.withBody(body);
try {
    CreateFirewallTagResponse response = client.createFirewallTag(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrMsg());
}
}
```

Python

Add a tag to a network ACL. Set the tag key to **key4** and tag value to **value4**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.valueOf("<YOUR REGION>")) \
        .build()

    try:
        request = CreateFirewallTagRequest()
        request.firewall_id = "{firewall_id}"
        tagbody = ResourceTag(
            key="key4",
            value="value4"
        )
        request.body = CreateFirewallTagRequestBody(
            tag=tagbody
        )
        response = client.create_firewall_tag(request)
        print(response)
    except exceptions.ClientRequestException as e:
```



```
print(e.status_code)
print(e.request_id)
print(e.error_code)
print(e.error_msg)
```

Go

Add a tag to a network ACL. Set the tag key to **key4** and tag value to **value4**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateFirewallTagRequest{}
    request.FirewallId = "{firewall_id}"
    tagbody := &model.ResourceTag{
        Key: "key4",
        Value: "value4",
    }
    request.Body = &model.CreateFirewallTagRequestBody{
        Tag: tagbody,
    }
    response, err := client.CreateFirewallTag(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
204	Normal request response. For more status codes, see Status Codes .

Error Codes

See [Error Codes](#).

5.10.4 Deleting 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.

Calling Method

For details, see [Calling APIs](#).

URI

DELETE /v3/{project_id}/firewalls/{firewall_id}/tags/{tag_key}

Table 5-309 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: 204

Normal request response. For more status codes, see [Status Codes](#).

None

Example Requests

Delete a tag from a network ACL.

```
DELETE https://{Endpoint}/v3/{project_id}/firewalls/{firewall_id}/tags/{tag_key}
```

Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class DeleteFirewallTagSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();

        DeleteFirewallTagRequest request = new DeleteFirewallTagRequest();
        request.withFirewallId("{firewall_id}");
        request.withTagKey("{tag_key}");
        try {
            DeleteFirewallTagResponse response = client.deleteFirewallTag(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
        }
    }
}
```

```
        System.out.println(e.getStatusCode());
        System.out.println(e.getRequestId());
        System.out.println(e.getErrorCode());
        System.out.println(e.getErrorMsg());
    }
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteFirewallTagRequest()
        request.firewall_id = "{firewall_id}"
        request.tag_key = "{tag_key}"
        response = client.delete_firewall_tag(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"
```

```
auth := basic.NewCredentialsBuilder().
    WithAk(ak).
    WithSk(sk).
    WithProjectId(projectId).
    Build()

client := vpc.NewVpcClient(
    vpc.VpcClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.DeleteFirewallTagRequest{}
request.FirewallId = "{firewall_id}"
request.TagKey = "{tag_key}"
response, err := client.DeleteFirewallTag(request)
if err == nil {
    fmt.Printf("%v\n", response)
} else {
    fmt.Println(err)
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
204	Normal request response. For more status codes, see Status Codes .

Error Codes

See [Error Codes](#).

5.10.5 Querying Tags of a Network ACL

Function

This API is used to query tags of a specific network ACL.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v3/{project_id}/firewalls/{firewall_id}/tags

Table 5-310 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 5-311 Response body parameters

Parameter	Type	Description
tags	Array of ResourceTag objects	Tags
request_id	String	Request ID

Table 5-312 ResourceTag

Parameter	Type	Description
key	String	- Tag key - Tag keys must be unique for each resource. - The value can contain 1 to 128 characters. Minimum: 1 Maximum: 128
value	String	- Tag value. - The value can contain no more than 255 characters Maximum: 255

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"
  } ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class ShowFirewallTagsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();
        ShowFirewallTagsRequest request = new ShowFirewallTagsRequest();
        request.withFirewallId("{firewall_id}");
        try {
            ShowFirewallTagsResponse response = client.showFirewallTags(request);
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

```
        System.out.println(response.toString());
    } catch (ConnectionException e) {
        e.printStackTrace();
    } catch (RequestTimeoutException e) {
        e.printStackTrace();
    } catch (ServiceResponseException e) {
        e.printStackTrace();
        System.out.println(e.getHttpStatusCode());
        System.out.println(e.getRequestId());
        System.out.println(e.getErrorCode());
        System.out.println(e.getErrorMsg());
    }
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowFirewallTagsRequest()
        request.firewall_id = "{firewall_id}"
        response = client.show_firewall_tags(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
```



```
// In this example, AK and SK are stored in environment variables for authentication. Before running this
example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak := os.Getenv("CLOUD_SDK_AK")
sk := os.Getenv("CLOUD_SDK_SK")
projectId := "{project_id}"

auth := basic.NewCredentialsBuilder().
    WithAk(ak).
    WithSk(sk).
    WithProjectId(projectId).
    Build()

client := vpc.NewVpcClient(
    vpc.VpcClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.ShowFirewallTagsRequest{}
request.FirewallId = "{firewall_id}"
response, err := client.ShowFirewallTags(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Normal response to the GET operation

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.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v3/{project_id}/firewalls/{firewall_id}/tags/create

Table 5-313 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 5-314 Request body parameters

Parameter	Mandatory	Type	Description
tags	Yes	Array of ResourceTag objects	Tags

Table 5-315 ResourceTag

Parameter	Mandatory	Type	Description
key	Yes	String	- Tag key - Tag keys must be unique for each resource. - The value can contain 1 to 128 characters. Minimum: 1 Maximum: 128
value	Yes	String	- Tag value. - The value can contain no more than 255 characters Maximum: 255

Response Parameters

Status code: 204

Normal request response. For more status codes, see [Status Codes](#).

None

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

SDK Sample Code

The SDK sample code is as follows.

Java

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**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

import java.util.List;
import java.util.ArrayList;

public class BatchCreateFirewallTagsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);
```

```
VpcClient client = VpcClient.newBuilder()
    .withCredential(auth)
    .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
    .build();
BatchCreateFirewallTagsRequest request = new BatchCreateFirewallTagsRequest();
request.withFirewallId("{firewall_id}");
BatchCreateFirewallTagsRequestBody body = new BatchCreateFirewallTagsRequestBody();
List<ResourceTag> listbodyTags = new ArrayList<>();
listbodyTags.add(
    new ResourceTag()
        .withKey("keyxxx")
        .withValue("value1")
);
listbodyTags.add(
    new ResourceTag()
        .withKey("keyyyy")
        .withValue("value2")
);
body.withTags(listbodyTags);
request.withBody(body);
try {
    BatchCreateFirewallTagsResponse response = client.batchCreateFirewallTags(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

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**.

coding: utf-8

```
import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *
```

```
if __name__ == "__main__":
```

```
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
```

```
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
```

```
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"
```

```
    credentials = BasicCredentials(ak, sk, projectId)
```

```
    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.valueOf("<YOUR REGION>")) \
        .build()
```

```
    try:
```

```
request = BatchCreateFirewallTagsRequest()
request.firewall_id = "{firewall_id}"
listTagsbody = [
    ResourceTag(
        key="keyxxx",
        value="value1"
    ),
    ResourceTag(
        key="keyyyy",
        value="value2"
    )
]
request.body = BatchCreateFirewallTagsRequestBody(
    tags=listTagsbody
)
response = client.batch_create_firewall_tags(request)
print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

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**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.BatchCreateFirewallTagsRequest{}
    request.FirewallId = "{firewall_id}"
    var listTagsbody = []model.ResourceTag{
        {
            Key: "keyxxx",
            Value: "value1",
        },
        {
            Key: "keyyyy",
```

```
        Value: "value2",
    },
}
request.Body = &model.BatchCreateFirewallTagsRequestBody{
    Tags: listTagsbody,
}
response, err := client.BatchCreateFirewallTags(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
204	Normal request response. For more status codes, see Status Codes .

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.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v3/{project_id}/firewalls/{firewall_id}/tags/delete

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
tags	Yes	Array of DeleteResourceTagRequestBody objects	Tags

Table 5-318 DeleteResourceTagRequestBody

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. The key of the same resource must be unique. Minimum: 1 Maximum: 128
value	No	String	Tag key Maximum: 255

Response Parameters

Status code: 204

Normal request response. For more status codes, see [Status Codes](#).

None

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

SDK Sample Code

The SDK sample code is as follows.

Java

Delete tags from a network ACL in batches. The key of the tag is **keyxxx**, and the value is **value1**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

import java.util.List;
import java.util.ArrayList;

public class BatchDeleteFirewallTagsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();
        BatchDeleteFirewallTagsRequest request = new BatchDeleteFirewallTagsRequest();
        request.withFirewallId("{firewall_id}");
        BatchDeleteFirewallTagsRequestBody body = new BatchDeleteFirewallTagsRequestBody();
```



```
List<DeleteResourceTagRequestBody> listbodyTags = new ArrayList<>();
listbodyTags.add(
    new DeleteResourceTagRequestBody()
        .withKey("keyxxx")
        .withValue("value1")
);
body.withTags(listbodyTags);
request.withBody(body);
try {
    BatchDeleteFirewallTagsResponse response = client.batchDeleteFirewallTags(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

Delete tags from a network ACL in batches. The key of the tag is **keyxxx**, and the value is **value1**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = BatchDeleteFirewallTagsRequest()
        request.firewall_id = "{firewall_id}"
        listTagsbody = [
            DeleteResourceTagRequestBody(
                key="keyxxx",
                value="value1"
            )
        ]
        request.body = BatchDeleteFirewallTagsRequestBody(
            tags=listTagsbody
        )
        response = client.batch_delete_firewall_tags(request)
        print(response)
```

```
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

Delete tags from a network ACL in batches. The key of the tag is **keyxxx**, and the value is **value1**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.BatchDeleteFirewallTagsRequest{}
    request.FirewallId = "{firewall_id}"
    valueTags := "value1"
    var listTagsbody = []model.DeleteResourceTagRequestBody{
        {
            Key: "keyxxx",
            Value: &valueTags,
        },
    }
    request.Body = &model.BatchDeleteFirewallTagsRequestBody{
        Tags: listTagsbody,
    }
    response, err := client.BatchDeleteFirewallTags(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
204	Normal request response. For more status codes, see Status Codes .

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.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v3/{project_id}/firewalls/tags

Table 5-319 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 5-320 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records to be queried. Minimum: 1 Maximum: 1000 Default: 1000

Parameter	Mandatory	Type	Description
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 5-321 Response body parameters

Parameter	Type	Description
tags	Array of ListTag objects	Tags
request_id	String	Request ID.
total_count	Integer	Resource quantity.

Table 5-322 ListTag

Parameter	Type	Description
key	String	Tag key. The key cannot be left blank. 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: 255

Example Requests

Query tags of network ACLs by project ID.

```
GET https://{Endpoint}/v3/{project_id}/firewalls/tags
```

Example Responses

Status code: 200

Normal request response. For more status codes, see [Status Codes](#).

```
{
  "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" ]
  } ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

public class ListFirewallTagsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
```

```
.withProjectId(projectId)
.withAk(ak)
.withSk(sk);

VpcClient client = VpcClient.newBuilder()
    .withCredential(auth)
    .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
    .build();
ListFirewallTagsRequest request = new ListFirewallTagsRequest();
try {
    ListFirewallTagsResponse response = client.listFirewallTags(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
    # In this example, AK and SK are stored in environment variables for authentication. Before running this
    # example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"

    credentials = BasicCredentials(ak, sk, projectId)

    client = VpcClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(VpcRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListFirewallTagsRequest()
        response = client.list_firewall_tags(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

Go

```
package main

import (
    "fmt"
```

```
"github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
"github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListFirewallTagsRequest{}
    response, err := client.ListFirewallTags(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Normal request response. For more status codes, see Status Codes .

Error Codes

See [Error Codes](#).

5.11 Port

5.11.1 Adding a Security Group to the Security Group List of a Port

Function

This API is used to add a security group to the security group list of a port.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v3/{project_id}/ports/{port_id}/insert-security-groups

Table 5-323 Path Parameters

Parameter	Mandatory	Type	Description
port_id	Yes	String	Unique identifier of a port.
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see Obtaining a Project ID .

Request Parameters

Table 5-324 Request body parameters

Parameter	Mandatory	Type	Description
port	Yes	InsertSecurityGroupOption object	Request body for inserting a security group to the security group list of a port.

Table 5-325 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. Examples are as follows: - To add a security group to the top of the associated security group list, set index to 0. - To add a security group after the <i>n</i>th security group in the associated security group list, set index to <i>n</i>. 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 5-326 Response body parameters

Parameter	Type	Description
request_id	String	Request ID.
port	Port object	Response body for inserting a security group to the security group list of a port.

Table 5-327 Port

Parameter	Type	Description
admin_state_up	Boolean	Administrative status. Value range: true or false Default value: true
binding:host_id	String	Host ID. Constraints: This parameter is visible only to administrators.
binding:profile	Object	User-defined settings.

Parameter	Type	Description
binding:vif_details	Object	Details about the virtual interface. ovs_hybrid_plug specifies whether the OVS/bridge hybrid mode is used.
binding:vif_type	String	Interface type of the port. The value can be ovs , hw_veb , or others. This is an extended attribute. Constraints: This parameter is visible only to administrators.
binding:vnic_type	String	Type of the bound vNIC. The value can be: - normal : software switching. - direct : SR-IOV PCIe passthrough. direct is not supported.
created_at	String	Time when the port was created. The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ss</i> .
updated_at	String	Time when the port was created. The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ss</i> .
description	String	Supplementary information about a port. The value can contain up to 255 characters and cannot contain angle brackets (< or >).
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.
device_owner	String	Device that a port belongs to, which can be a DHCP server, router, load balancer, or Nova.
ecs_flavor	String	Flavor of the ECS that the port belongs to.
id	String	Port ID, which uniquely identifies a port. The value must be in standard UUID format.

Parameter	Type	Description
instance_id	String	ID of the instance that the port belongs to, for example, RDS instance ID. The system automatically sets this parameter.
instance_type	String	Type of the instance that the port belongs to, for example, RDS. The system automatically sets this parameter.
mac_address	String	MAC address.
name	String	Port name. The value can contain no more than 255 characters. This parameter is left blank by default.
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. Value range: true or false
private_ips	Array of PrivateIpInfo objects	Private IP address of the port.
project_id	String	Project ID. The value must be in standard UUID format.
security_groups	Array of strings	Security groups associated with the port.
status	String	Port status. The value can be ACTIVE , BUILD , or DOWN .
tenant_id	String	Tenant ID. The value must be in standard UUID format.
virsubnet_id	String	Network ID. The value must be in standard UUID format.
vpc_id	String	VPC ID. The value must be in standard UUID format.

Parameter	Type	Description
vpc_tenant_id	String	VPC tenant ID. The value must be in standard UUID format.
vtep_ip	String	VTEP IP address.
enable_efi	Boolean	Whether to enable efi . If efi is enabled, the port supports vRoCE. Value range: true or false Default value: false
scope	String	Application scope. The value can be: • center: central AZs. • {azId}: specific AZs. Default value: center
zone_id	String	AZ that the port belongs to.
binding:migration_info	Object	Destination node information, including the details defined by binding:vif_details and binding:vif_type .
extra_dhcp_opts	Array of ExtraDhcpOpt objects	Extended attributes of DHCP.
position_type	String	Location type in the edge scenario. Default value: center
instance_info	Object	Information about the instance bound to the port.
tags	Array of strings	Port tags.

Parameter	Type	Description
allowed_address_pairs	Array of AllowedAddressPair objects	IP address and MAC address pairs. Constraints: • The IP address cannot be 0.0.0.0/0. • Configure a dedicated security group for the port if allowed_address_pairs has a CIDR block with a netmask length 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.

Table 5-328 PrivateIpInfo

Parameter	Type	Description
subnet_cidr_id	String	ID of the subnet where the port works.
ip_address	String	Private IP address of the port.

Table 5-329 ExtraDhcpOpt

Parameter	Type	Description
opt_name	String	Option name.
opt_value	String	Option value.

Table 5-330 AllowedAddressPair

Parameter	Type	Description
ip_address	String	Definition: IP address. Constraints: Configure a dedicated security group if a large CIDR block (subnet mask less than 24) is configured for parameter allowed_address_pairs . Range: Single IP address, for example, 192.168.21.25 A CIDR block, for example, 192.168.21.0/24 Default Value: N/A
mac_address	String	Definition: MAC address. Constraints: N/A Range: N/A Default Value: N/A

Example Requests

Add a security group above 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 Responses

Status code: 200
Normal response to the PUT operation. For more status codes, see [Status Codes](#).

```
{
  "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": "",
    "zone_id": "",
    "scope": "center",
    "position_type": "center",
    "created_at": "2023-05-10T01:35:02.000+00:00",
    "updated_at": "2023-05-10T01:35:02.000+00:00",
    "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_id": "",
    "instance_type": "",
    "ecs_flavor": "",
    "enable_efa": false,
    "vpc_subnet_id": "3847b263-2370-45c0-8236-38a1de568049",
    "private_ips": [ {
      "subnet_cidr_id": "ffe98087-6d4f-45cd-988b-1c87f75d2d53",
      "ip_address": "192.168.158.228"
    } ],
    "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"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Add a security group above 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**.

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

import java.util.List;
import java.util.ArrayList;
```

```
public class AddSecurityGroupsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
        // security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or
        // environment variables and decrypted during use to ensure security.
        // In this example, AK and SK are stored in environment variables for authentication. Before running
        // this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
        String ak = System.getenv("CLOUD_SDK_AK");
        String sk = System.getenv("CLOUD_SDK_SK");
        String projectId = "{project_id}";

        ICredential auth = new BasicCredentials()
            .withProjectId(projectId)
            .withAk(ak)
            .withSk(sk);

        VpcClient client = VpcClient.newBuilder()
            .withCredential(auth)
            .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
            .build();

        AddSecurityGroupsRequest request = new AddSecurityGroupsRequest();
        request.withPortId("{port_id}");
        AddSecurityGroupsRequestBody body = new AddSecurityGroupsRequestBody();
        List<String> listPortSecurityGroups = new ArrayList<>();
        listPortSecurityGroups.add("8edd3747-ccd4-49a1-82b9-a165eec314b4");
        listPortSecurityGroups.add("6c2d4540-3b7d-4207-a319-a7231b439995");
        InsertSecurityGroupOption portbody = new InsertSecurityGroupOption();
        portbody.withSecurityGroups(listPortSecurityGroups)
            .withIndex(1);
        body.withPort(portbody);
        request.withBody(body);
        try {
            AddSecurityGroupsResponse response = client.addSecurityGroups(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getHttpStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

Add a security group above 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**.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *

if __name__ == "__main__":
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    # risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    # variables and decrypted during use to ensure security.
```



```
# In this example, AK and SK are stored in environment variables for authentication. Before running this
example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
ak = os.environ["CLOUD_SDK_AK"]
sk = os.environ["CLOUD_SDK_SK"]
projectId = "{project_id}"

credentials = BasicCredentials(ak, sk, projectId)

client = VpcClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(VpcRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = AddSecurityGroupsRequest()
    request.port_id = "{port_id}"
    listSecurityGroupsPort = [
        "8edd3747-ccd4-49a1-82b9-a165eec314b4",
        "6c2d4540-3b7d-4207-a319-a7231b439995"
    ]
    portbody = InsertSecurityGroupOption(
        security_groups=listSecurityGroupsPort,
        index=1
    )
    request.body = AddSecurityGroupsRequestBody(
        port=portbody
    )
    response = client.add_security_groups(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

Add a security group above 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**.

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()
```

```
client := vpc.NewVpcClient(  
    vpc.VpcClientBuilder().  
        WithRegion(region.ValueOf("<YOUR REGION>")).  
        WithCredential(auth).  
        Build())  
  
request := &model.AddSecurityGroupsRequest{  
    request.PortId = "{port_id}"  
    var listSecurityGroupsPort = []string{  
        "8edd3747-ccd4-49a1-82b9-a165eec314b4",  
        "6c2d4540-3b7d-4207-a319-a7231b439995",  
    }  
    indexPort:= int32(1)  
    portbody := &model.InsertSecurityGroupOption{  
        SecurityGroups: listSecurityGroupsPort,  
        Index: &indexPort,  
    }  
    request.Body = &model.AddSecurityGroupsRequestBody{  
        Port: portbody,  
    }  
    response, err := client.AddSecurityGroups(request)  
    if err == nil {  
        fmt.Printf("%v\n", response)  
    } else {  
        fmt.Println(err)  
    }  
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Normal response to the PUT operation. For more status codes, see Status Codes .

Error Codes

See [Error Codes](#).

5.11.2 Removing a Security Group from the Security Group List of a Port

Function

This API is used to remove a security group from the security group list of a port.

Calling Method

For details, see [Calling APIs](#).

URI

PUT /v3/{project_id}/ports/{port_id}/remove-security-groups

Table 5-331 Path Parameters

Parameter	Mandatory	Type	Description
port_id	Yes	String	Unique identifier of a port.
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see Obtaining a Project ID .

Request Parameters

Table 5-332 Request body parameters

Parameter	Mandatory	Type	Description
port	Yes	RemoveSecurityGroupOption object	Request body for removing a security group from a security group list of a port.

Table 5-333 RemoveSecurityGroupOption

Parameter	Mandatory	Type	Description
security_groups	Yes	Array of strings	Security group IDs, for example, "security_groups": ["a0608cbf-d047-4f54-8b28-cd7b59853fff"].

Response Parameters

Status code: 200

Table 5-334 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 5-335 Port

Parameter	Type	Description
admin_state_up	Boolean	Administrative status. Value range: true or false Default value: true
binding:host_id	String	Host ID. Constraints: This parameter is visible only to administrators.
binding:profile	Object	User-defined settings.
binding:vif_details	Object	Details about the virtual interface. ovs_hybrid_plug specifies whether the OVS/bridge hybrid mode is used.
binding:vif_type	String	Interface type of the port. The value can be ovs , hw_veb , or others. This is an extended attribute. Constraints: This parameter is visible only to administrators.
binding:vnic_type	String	Type of the bound vNIC. The value can be: - normal : software switching. - direct : SR-IOV PCIe passthrough. direct is not supported.
created_at	String	Time when the port was created. The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ss</i> .
updated_at	String	Time when the port was created. The value is a UTC time in the format of <i>yyyy-MM-ddTHH:mm:ss</i> .
description	String	Supplementary information about a port. The value can contain up to 255 characters and cannot contain angle brackets (< or >).
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.

Parameter	Type	Description
device_owner	String	Device that a port belongs to, which can be a DHCP server, router, load balancer, or Nova.
ecs_flavor	String	Flavor of the ECS that the port belongs to.
id	String	Port ID, which uniquely identifies a port. The value must be in standard UUID format.
instance_id	String	ID of the instance that the port belongs to, for example, RDS instance ID. The system automatically sets this parameter.
instance_type	String	Type of the instance that the port belongs to, for example, RDS. The system automatically sets this parameter.
mac_address	String	MAC address.
name	String	Port name. The value can contain no more than 255 characters. This parameter is left blank by default.
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. Value range: true or false
private_ips	Array of PrivateIpInfo objects	Private IP address of the port.
project_id	String	Project ID. The value must be in standard UUID format.
security_groups	Array of strings	Security groups associated with the port.
status	String	Port status. The value can be ACTIVE , BUILD , or DOWN .

Parameter	Type	Description
tenant_id	String	Tenant ID. The value must be in standard UUID format.
virsubnet_id	String	Network ID. The value must be in standard UUID format.
vpc_id	String	VPC ID. The value must be in standard UUID format.
vpc_tenant_id	String	VPC tenant ID. The value must be in standard UUID format.
vtep_ip	String	VTEP IP address.
enable_efi	Boolean	Whether to enable efi . If efi is enabled, the port supports vRoCE. Value range: true or false Default value: false
scope	String	Application scope. The value can be: • center: central AZs. • {azId}: specific AZs. Default value: center
zone_id	String	AZ that the port belongs to.
binding:migration_info	Object	Destination node information, including the details defined by binding:vif_details and binding:vif_type .
extra_dhcp_opts	Array of ExtraDhcpOpt objects	Extended attributes of DHCP.
position_type	String	Location type in the edge scenario. Default value: center
instance_info	Object	Information about the instance bound to the port.
tags	Array of strings	Port tags.

Parameter	Type	Description
allowed_address_pairs	Array of AllowedAddressPair objects	IP address and MAC address pairs. Constraints: • The IP address cannot be 0.0.0.0/0. • Configure a dedicated security group for the port if allowed_address_pairs has a CIDR block with a netmask length 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.

Table 5-336 PrivateIpInfo

Parameter	Type	Description
subnet_cidr_id	String	ID of the subnet where the port works.
ip_address	String	Private IP address of the port.

Table 5-337 ExtraDhcpOpt

Parameter	Type	Description
opt_name	String	Option name.
opt_value	String	Option value.

Table 5-338 AllowedAddressPair

Parameter	Type	Description
ip_address	String	Definition: IP address. Constraints: Configure a dedicated security group if a large CIDR block (subnet mask less than 24) is configured for parameter allowed_address_pairs . Range: Single IP address, for example, 192.168.21.25 A CIDR block, for example, 192.168.21.0/24 Default Value: N/A
mac_address	String	Definition: MAC address. Constraints: N/A Range: N/A Default Value: N/A

Example Requests

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 Responses

Status code: 200

Normal response to the PUT operation. For more status codes, see [Status Codes](#).

```
{
  "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" : "",
"zone_id" : "",
"scope" : "center",
"position_type" : "center",
"created_at" : "2023-05-10T01:35:02.000+00:00",
"updated_at" : "2023-05-10T01:35:02.000+00:00",
"port_security_enabled" : true,
"tags" : [ ],
"security_groups" : [ "567be4e3-d171-46ce-9e8a-c15e91cfe86a", "4940b983-5992-4663-bed9-d1d1e15d1009" ],
"allowed_address_pairs" : [ ],
"extra_dhcp_opts" : [ ],
"instance_id" : "",
"instance_type" : "",
"ecs_flavor" : "",
"enable_efa" : false,
"vpc_subnet_id" : "3847b263-2370-45c0-8236-38a1de568049",
"private_ips" : [ {
  "subnet_cidr_id" : "ffe98087-6d4f-45cd-988b-1c87f75d2d53",
  "ip_address" : "192.168.158.228"
} ],
"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"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Remove security groups (**8edd3747-ccd4-49a1-82b9-a165eec314b4** and **6c2d4540-3b7d-4207-a319-a7231b439995**) associated with the port (**99fd0c77-56b4-4bf6-8365-df352e45d5fc**).

```
package com.huaweicloud.sdk.test;

import com.huaweicloud.sdk.core.auth.ICredential;
import com.huaweicloud.sdk.core.auth.BasicCredentials;
import com.huaweicloud.sdk.core.exception.ConnectionException;
import com.huaweicloud.sdk.core.exception.RequestTimeoutException;
import com.huaweicloud.sdk.core.exception.ServiceResponseException;
import com.huaweicloud.sdk.vpc.v3.region.VpcRegion;
import com.huaweicloud.sdk.vpc.v3.*;
import com.huaweicloud.sdk.vpc.v3.model.*;

import java.util.List;
import java.util.ArrayList;

public class RemoveSecurityGroupsSolution {

    public static void main(String[] args) {
        // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great
```

security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.

// In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment

```
String ak = System.getenv("CLOUD_SDK_AK");
String sk = System.getenv("CLOUD_SDK_SK");
String projectId = "{project_id}";
```

```
ICredential auth = new BasicCredentials()
    .withProjectId(projectId)
    .withAk(ak)
    .withSk(sk);
```

```
VpcClient client = VpcClient.newBuilder()
    .withCredential(auth)
    .withRegion(VpcRegion.valueOf("<YOUR REGION>"))
    .build();
```

```
RemoveSecurityGroupsRequest request = new RemoveSecurityGroupsRequest();
request.withPortId("{port_id}");
RemoveSecurityGroupsRequestBody body = new RemoveSecurityGroupsRequestBody();
List<String> listPortSecurityGroups = new ArrayList<>();
listPortSecurityGroups.add("8edd3747-ccd4-49a1-82b9-a165eec314b4");
listPortSecurityGroups.add("6c2d4540-3b7d-4207-a319-a7231b439995");
RemoveSecurityGroupOption portbody = new RemoveSecurityGroupOption();
portbody.withSecurityGroups(listPortSecurityGroups);
body.withPort(portbody);
request.withBody(body);
try {
    RemoveSecurityGroupsResponse response = client.removeSecurityGroups(request);
    System.out.println(response.toString());
} catch (ConnectionException e) {
    e.printStackTrace();
} catch (RequestTimeoutException e) {
    e.printStackTrace();
} catch (ServiceResponseException e) {
    e.printStackTrace();
    System.out.println(e.getHttpStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

Remove security groups (**8edd3747-ccd4-49a1-82b9-a165eec314b4** and **6c2d4540-3b7d-4207-a319-a7231b439995**) associated with the port (**99fd0c77-56b4-4bf6-8365-df352e45d5fc**).

```
# coding: utf-8
```

```
import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkvpc.v3.region.vpc_region import VpcRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkvpc.v3 import *
```

```
if __name__ == "__main__":
```

```
    # The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment variables and decrypted during use to ensure security.
```

```
    # In this example, AK and SK are stored in environment variables for authentication. Before running this example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
```

```
    ak = os.environ["CLOUD_SDK_AK"]
    sk = os.environ["CLOUD_SDK_SK"]
    projectId = "{project_id}"
```

```
credentials = BasicCredentials(ak, sk, projectId)

client = VpcClient.new_builder() \
    .with_credentials(credentials) \
    .with_region(VpcRegion.value_of("<YOUR REGION>")) \
    .build()

try:
    request = RemoveSecurityGroupsRequest()
    request.port_id = "{port_id}"
    listSecurityGroupsPort = [
        "8edd3747-ccd4-49a1-82b9-a165eec314b4",
        "6c2d4540-3b7d-4207-a319-a7231b439995"
    ]
    portbody = RemoveSecurityGroupOption(
        security_groups=listSecurityGroupsPort
    )
    request.body = RemoveSecurityGroupsRequestBody(
        port=portbody
    )
    response = client.remove_security_groups(request)
    print(response)
except exceptions.ClientRequestException as e:
    print(e.status_code)
    print(e.request_id)
    print(e.error_code)
    print(e.error_msg)
```

Go

Remove security groups (**8edd3747-ccd4-49a1-82b9-a165eec314b4** and **6c2d4540-3b7d-4207-a319-a7231b439995**) associated with the port (**99fd0c77-56b4-4bf6-8365-df352e45d5fc**).

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    vpc "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/vpc/v3/region"
)

func main() {
    // The AK and SK used for authentication are hard-coded or stored in plaintext, which has great security
    // risks. It is recommended that the AK and SK be stored in ciphertext in configuration files or environment
    // variables and decrypted during use to ensure security.
    // In this example, AK and SK are stored in environment variables for authentication. Before running this
    // example, set environment variables CLOUD_SDK_AK and CLOUD_SDK_SK in the local environment
    ak := os.Getenv("CLOUD_SDK_AK")
    sk := os.Getenv("CLOUD_SDK_SK")
    projectId := "{project_id}"

    auth := basic.NewCredentialsBuilder().
        WithAk(ak).
        WithSk(sk).
        WithProjectId(projectId).
        Build()

    client := vpc.NewVpcClient(
        vpc.VpcClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.RemoveSecurityGroupsRequest{
        request.PortId = "{port_id}"
    }
```

```
var listSecurityGroupsPort = []string{
    "8edd3747-ccd4-49a1-82b9-a165eec314b4",
    "6c2d4540-3b7d-4207-a319-a7231b439995",
}
portbody := &model.RemoveSecurityGroupOption{
    SecurityGroups: listSecurityGroupsPort,
}
request.Body = &model.RemoveSecurityGroupsRequestBody{
    Port: portbody,
}
response, err := client.RemoveSecurityGroups(request)
if err == nil {
    fmt.Printf("%+v\n", response)
} else {
    fmt.Println(err)
}
```

More

For SDK sample code of more programming languages, see the Sample Code tab in [API Explorer](#). SDK sample code can be automatically generated.

Status Codes

Status Code	Description
200	Normal response to the PUT operation. For more status codes, see Status Codes .

Error Codes

See [Error Codes](#).

5.12 Subnet CIDR Reservations

5.12.1 Creating a Subnet CIDR Reservation

Function

This API is used to create a subnet CIDR reservation.

Calling Method

For details, see [Calling APIs](#).

URI

POST /v3/{project_id}/vpc/virsubnet-cidr-reservations

Table 5-339 Path Parameters

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 5-340 Request body parameters

Parameter	Mandatory	Type	Description
dry_run	No	Boolean	- Whether to only send the check request. - The value can be: true: Only the check request will be sent and no subnet CIDR reservation will be created. Check items include mandatory parameters, request format, and constraints. 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 subnet CIDR reservation will be created.
virsubnet_cidr_reservation	Yes	CreateVirsubnetCidrReservationOption object	Request body for creating a subnet CIDR reservation.

Table 5-341 CreateVirsubnetCidrReservationOption

Parameter	Mandatory	Type	Description
virsubnet_id	Yes	String	ID of the virtual subnet that a subnet CIDR reservation belongs to.
ip_version	Yes	Integer	- IP version of a subnet CIDR reservation. Both IPv4 and IPv6 are supported. - The value can be: 4: IPv4 6: IPv6
cidr	No	String	- Subnet CIDR reservation. - The value is in CIDR block format. The minimum netmask value is the subnet netmask value plus 2, and the maximum netmask value is 32 (IPv4) or 128 (IPv6). - Note: - Either cidr or mask must be specified. If both are specified, the two values cannot conflict with each other. - A subnet CIDR reservation cannot contain the used IP addresses in the subnet and the reserved IP addresses by the system (the first and last two IP addresses in the subnet).

Parameter	Mandatory	Type	Description
mask	No	Integer	• Netmask value of a subnet CIDR reservation. • The value is an integer. The minimum netmask value is the subnet netmask value plus 2, and the maximum netmask value is 32 (IPv4) or 128 (IPv6). • Note: – Either cidr or mask must be specified. If both are specified, the two values cannot conflict with each other. – A subnet CIDR reservation cannot contain the used IP addresses in the subnet and the reserved IP addresses by the system (the first and last two IP addresses in the subnet). – If you specify a netmask length when creating a subnet CIDR reservation, the system automatically allocates the bits of the difference between the value of mask and the specified netmask. For example, if the subnet CIDR block is 192.168.21.0/24, the subnet netmask is 24, and the specified netmask is 27, the system automatically allocates bits 25, 26, and 27. – Bits 25 to 27 are allocated to 011. The subnet CIDR reservation is 192.168.21.96/27. 96 in binary is 0110 0000.

Parameter	Mandatory	Type	Description
			Bits 25 to 27 are allocated to 110. The subnet CIDR reservation is 192.168.21.192/27. 192 in binary is 1100 0000.
name	No	String	- Name of a subnet CIDR reservation. - The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	No	String	- Description of a subnet CIDR reservation. - The value can contain no more than 255 characters and cannot contain angle brackets (< or >).

Response Parameters

Status code: 201

Table 5-342 Response body parameters

Parameter	Type	Description
request_id	String	Request ID.
virsubnet_cidr_reservation	VirsubnetCidrReservation object	Response body for creating a subnet CIDR reservation.

Table 5-343 VirsubnetCidrReservation

Parameter	Type	Description
id	String	- Unique ID of a subnet CIDR reservation. - The value is in UUID format with hyphens (-).

Parameter	Type	Description
virsubnet_id	String	- ID of the virtual subnet that a subnet CIDR reservation belongs to. - The value is in UUID format with hyphens (-).
vpc_id	String	- ID of the VPC that a subnet CIDR reservation belongs to. - The value is in UUID format with hyphens (-).
ip_version	Integer	- IP version of a subnet CIDR reservation. - The value can be: 4: IPv4 6: IPv6
cidr	String	- Subnet CIDR reservation. - The value is in CIDR block format. The minimum netmask value is the subnet netmask value plus 2, and the maximum netmask value is 32 (IPv4) or 128 (IPv6).
name	String	- Name of a subnet CIDR reservation. - The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	- Description of a subnet CIDR reservation. - The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
project_id	String	ID of the project that a subnet CIDR reservation belongs to.
created_at	String	- The time when a subnet CIDR reservation is created. - UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
updated_at	String	- The time when a subnet CIDR reservation is updated. - UTC time in the format of yyyy-MM-ddTHH:mm:ssZ

Example Requests

Create a subnet CIDR reservation. The virtual subnet ID is fb0e2bd6-190f-0d1a-7728-a5f6b1d8dd19, the IPv4 version is used, the subnet CIDR reservation is 192.168.21.96/28, the name is **test**, and the description is **for test**.

```
POST https://{Endpoint}/v3/{project_id}/vpc/virsubnet-cidr-reservations
{
  "virsubnet_cidr_reservation": {
    "virsubnet_id": "fb0e2bd6-190f-0d1a-7728-a5f6b1d8dd19",
    "ip_version": 4,
    "cidr": "192.168.21.96/28",
    "name": "test",
    "description": "for test"
  }
}
```

Example Responses

Status code: 201

The POST operation is successful. For more status codes, see [Status Codes](#).

```
{
  "virsubnet_cidr_reservation": {
    "id": "ed4edb94-754c-7848-bb77-2d381906c535",
    "virsubnet_id": "fb0e2bd6-190f-0d1a-7728-a5f6b1d8dd19",
    "vpc_id": "cef5d621-6c20-d5df-74e8-746271fba734",
    "ip_version": 4,
    "cidr": "192.168.21.96/28",
    "name": "test",
    "description": "for test",
    "project_id": "11e8dd119c77479db890e266e68c1ecf",
    "created_at": "2024-09-09T11:56:27Z",
    "updated_at": "2024-09-09T11:56:27Z",
  },
  "request_id": "fd48620df5f57b04917f2cc5ebeaf277"
}
```

Status Codes

Status Code	Description
201	The POST operation is successful. For more status codes, see Status Codes .

Error Codes

See [Error Codes](#).

5.12.2 Querying the List of Subnet CIDR Reservations

Function

This API is used to query the list of subnet CIDR reservations of a tenant.

Constraints

You can query all subnet CIDR reservations under your account. A maximum of 2,000 records can be returned for each query. If the number of records exceeds 2,000, the pagination marker will be returned.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v3/{project_id}/vpc/virsubnet-cidr-reservations

Table 5-344 Path Parameters

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 5-345 Query Parameters

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.
id	No	Array of strings	ID of a subnet CIDR reservation. This parameter can be used to filter subnet CIDR reservations. Multiple IDs can be specified.
virsubnet_id	No	Array of strings	ID of the virtual subnet that a subnet CIDR reservation belongs to. This parameter can be used to filter subnet CIDR reservations. Multiple IDs can be specified.

Parameter	Mandatory	Type	Description
cidr	No	Array of strings	Subnet CIDR reservation. This parameter can be used to filter subnet CIDR reservations. Multiple CIDR blocks can be specified.
ip_version	No	Array of integers	- IP version of the subnet that a subnet CIDR reservation belongs to. This parameter can be used to filter subnet CIDR reservations. - The value can be 4 or 6.
name	No	Array of strings	Name of a subnet CIDR reservation. This parameter can be used to filter subnet CIDR reservations. Multiple names can be specified.
description	No	Array of strings	Description of a subnet CIDR reservation. This parameter can be used to filter subnet CIDR reservations. Multiple descriptions can be specified.
enterprise_project_id	No	String	- Enterprise project ID. This parameter is used to filter subnet CIDR reservations of an enterprise project. - The project ID can be 0 or a string that contains a maximum of 36 characters in UUID format with hyphens (-). 0 indicates the default enterprise project. - To obtain the subnet CIDR reservations associated with all enterprise projects, specify all_granted_eps.

Request Parameters

None

Response Parameters

Status code: 200

Table 5-346 Response body parameters

Parameter	Type	Description
virsubnet_cidr_reservations	Array of VirsubnetCidrReservation objects	Response body of the subnet CIDR reservation list.
request_id	String	Request ID.
page_info	PageInfo object	Pagination information.

Table 5-347 VirsubnetCidrReservation

Parameter	Type	Description
id	String	- Unique ID of a subnet CIDR reservation. - The value is in UUID format with hyphens (-).
virsubnet_id	String	- ID of the virtual subnet that a subnet CIDR reservation belongs to. - The value is in UUID format with hyphens (-).
vpc_id	String	- ID of the VPC that a subnet CIDR reservation belongs to. - The value is in UUID format with hyphens (-).
ip_version	Integer	- IP version of a subnet CIDR reservation. - The value can be: 4: IPv4 6: IPv6
cidr	String	- Subnet CIDR reservation. - The value is in CIDR block format. The minimum netmask value is the subnet netmask value plus 2, and the maximum netmask value is 32 (IPv4) or 128 (IPv6).
name	String	- Name of a subnet CIDR reservation. - The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).

Parameter	Type	Description
description	String	• Description of a subnet CIDR reservation. • The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
project_id	String	• ID of the project that a subnet CIDR reservation belongs to.
created_at	String	• The time when a subnet CIDR reservation is created. • UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
updated_at	String	• The time when a subnet CIDR reservation is updated. • UTC time in the format of yyyy-MM-ddTHH:mm:ssZ

Table 5-348 PageInfo

Parameter	Type	Description
previous_marker	String	Definition: The first record on the current page. Range: N/A
current_count	Integer	Definition: Total number of resources on the current page. Range: N/A
next_marker	String	Definition: The last record on the current page. The next_marker field does not exist if the page is the last one. Range: N/A

Example Requests

Query the list of subnet CIDR reservations.

```
GET https://{Endpoint}/v3/{project_id}/vpc/virsubnet-cidr-reservations
```

Example Responses

Status code: 200

The GET operation is successful. For more status codes, see [Status Codes](#).

```
{
  "virsubnet_cidr_reservations": [
    {
      "id": "987d7959-9c48-ad49-2fdd-bf4146d6ebc4",
      "virsubnet_id": "fb0e2bd6-190f-0d1a-7728-a5f6b1d8dd19",
      "vpc_id": "cef5d621-6c20-d5df-74e8-746271fba734",
      "ip_version": 4,
      "cidr": "192.168.21.96/28",
      "name": "test",
      "description": "for test",
      "project_id": "11e8dd119c77479db890e266e68c1ecf",
      "created_at": "2024-09-09T10:20:35Z",
      "updated_at": "2024-09-09T10:20:35Z",
    },
    {
      "id": "ed4edb94-754c-7848-bb77-2d381906c535",
      "virsubnet_id": "fb0e2bd6-190f-0d1a-7728-a5f6b1d8dd19",
      "vpc_id": "cef5d621-6c20-d5df-74e8-746271fba734",
      "ip_version": 4,
      "cidr": "192.168.21.128/27",
      "name": "test2",
      "description": "for test",
      "project_id": "11e8dd119c77479db890e266e68c1ecf",
      "created_at": "2024-09-09T11:56:27Z",
      "updated_at": "2024-09-09T11:56:27Z",
    }
  ],
  "page_info": {
    "previous_marker": "987d7959-9c48-ad49-2fdd-bf4146d6ebc4",
    "current_count": 2
  },
  "request_id": "5cd6bbc22313ccb6933540d6f9302d81"
}
```

Status Codes

Status Code	Description
200	The GET operation is successful. For more status codes, see Status Codes .

Error Codes

See [Error Codes](#).

5.12.3 Querying Details About a Subnet CIDR Reservation

Function

This API is used to query details about a single subnet CIDR reservation.

Calling Method

For details, see [Calling APIs](#).

URI

GET /v3/{project_id}/vpc/virsubnet-cidr-reservations/{virsubnet_cidr_reservation_id}

Table 5-349 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see Obtaining a Project ID .
virsubnet_cidr_reservation_id	Yes	String	ID of a subnet CIDR reservation.

Request Parameters

None

Response Parameters

Status code: 200

Table 5-350 Response body parameters

Parameter	Type	Description
request_id	String	Request ID.
virsubnet_cidr_reservation	VirsubnetCidrReservation object	Response body for querying details about a subnet CIDR reservation.

Table 5-351 VirsubnetCidrReservation

Parameter	Type	Description
id	String	- Unique ID of a subnet CIDR reservation. - The value is in UUID format with hyphens (-).

Parameter	Type	Description
virsubnet_id	String	- ID of the virtual subnet that a subnet CIDR reservation belongs to. - The value is in UUID format with hyphens (-).
vpc_id	String	- ID of the VPC that a subnet CIDR reservation belongs to. - The value is in UUID format with hyphens (-).
ip_version	Integer	- IP version of a subnet CIDR reservation. - The value can be: 4: IPv4 6: IPv6
cidr	String	- Subnet CIDR reservation. - The value is in CIDR block format. The minimum netmask value is the subnet netmask value plus 2, and the maximum netmask value is 32 (IPv4) or 128 (IPv6).
name	String	- Name of a subnet CIDR reservation. - The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	- Description of a subnet CIDR reservation. - The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
project_id	String	ID of the project that a subnet CIDR reservation belongs to.
created_at	String	- The time when a subnet CIDR reservation is created. - UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
updated_at	String	- The time when a subnet CIDR reservation is updated. - UTC time in the format of yyyy-MM-ddTHH:mm:ssZ

Example Requests

Query details about a subnet CIDR reservation.

```
GET https://{Endpoint}/v3/{project_id}/vpc/virsubnet-cidr-reservations/987d7959-9c48-ad49-2fdd-bf4146d6ebc4
```

Example Responses

Status code: 200

The GET operation is successful. For more status codes, see [Status Codes](#).

```
{
  "virsubnet_cidr_reservation": {
    "id": "987d7959-9c48-ad49-2fdd-bf4146d6ebc4",
    "virsubnet_id": "fb0e2bd6-190f-0d1a-7728-a5f6b1d8dd19",
    "vpc_id": "cef5d621-6c20-d5df-74e8-746271fba734",
    "ip_version": 4,
    "cidr": "192.168.21.96/28",
    "name": "test",
    "description": "for test",
    "project_id": "11e8dd119c77479db890e266e68c1ecf",
    "created_at": "2024-09-09T10:20:35Z",
    "updated_at": "2024-09-09T10:20:35Z"
  },
  "request_id": "96579891a62195d2c54054ac43fab0aa"
}
```

Status Codes

Status Code	Description
200	The GET operation is successful. For more status codes, see Status Codes .

Error Codes

See [Error Codes](#).

5.12.4 Updating a Subnet CIDR Reservation

Function

This API is used to update a subnet CIDR reservation.

Calling Method

For details, see [Calling APIs](#).

URI

```
PUT /v3/{project_id}/vpc/virsubnet-cidr-reservations/{virsubnet_cidr_reservation_id}
```

Table 5-352 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see Obtaining a Project ID .
virsubnet_cidr_reservation_id	Yes	String	ID of a subnet CIDR reservation.

Request Parameters

Table 5-353 Request body parameters

Parameter	Mandatory	Type	Description
dry_run	No	Boolean	- Whether to only send the check request. - The value can be: true: Only the check request will be sent and no subnet CIDR reservation will be updated. Check items include mandatory parameters, request format, and constraints. 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 subnet CIDR reservation will be updated.
virsubnet_cidr_reservation	Yes	UpdateVirusubnetCidrReservationOption object	Request body for updating a subnet CIDR reservation.

Table 5-354 UpdateVirsubnetCidrReservationOption

Parameter	Mandatory	Type	Description
name	No	String	- Name of a subnet CIDR reservation. - The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	No	String	- Description of a subnet CIDR reservation. - The value can contain no more than 255 characters and cannot contain angle brackets (< or >).

Response Parameters

Status code: 200

Table 5-355 Response body parameters

Parameter	Type	Description
request_id	String	Request ID.
virsubnet_cidr_reservation	VirsubnetCidrReservation object	Response body for updating a subnet CIDR reservation.

Table 5-356 VirsubnetCidrReservation

Parameter	Type	Description
id	String	- Unique ID of a subnet CIDR reservation. - The value is in UUID format with hyphens (-).
virsubnet_id	String	- ID of the virtual subnet that a subnet CIDR reservation belongs to. - The value is in UUID format with hyphens (-).

Parameter	Type	Description
vpc_id	String	- ID of the VPC that a subnet CIDR reservation belongs to. - The value is in UUID format with hyphens (-).
ip_version	Integer	- IP version of a subnet CIDR reservation. - The value can be: 4: IPv4 6: IPv6
cidr	String	- Subnet CIDR reservation. - The value is in CIDR block format. The minimum netmask value is the subnet netmask value plus 2, and the maximum netmask value is 32 (IPv4) or 128 (IPv6).
name	String	- Name of a subnet CIDR reservation. - The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	- Description of a subnet CIDR reservation. - The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
project_id	String	ID of the project that a subnet CIDR reservation belongs to.
created_at	String	- The time when a subnet CIDR reservation is created. - UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
updated_at	String	- The time when a subnet CIDR reservation is updated. - UTC time in the format of yyyy-MM-ddTHH:mm:ssZ

Example Requests

Update name and description of the subnet CIDR reservation whose ID is ed4edb94-754c-7848-bb77-2d381906c535 to **name-test-updated** and **description-test-updated**.

```
PUT https://{Endpoint}/v3/{project_id}/vpc/virsubnet-cidr-reservations/ed4edb94-754c-7848-bb77-2d381906c535

{
  "virsubnet_cidr_reservation": {
    "name": "name-test-updated",
    "description": "description-test-updated"
  }
}
```

Example Responses

Status code: 200

The PUT operation is successful. For more status codes, see [Status Codes](#).

```
{
  "virsubnet_cidr_reservation": {
    "id": "ed4edb94-754c-7848-bb77-2d381906c535",
    "virsubnet_id": "fb0e2bd6-190f-0d1a-7728-a5f6b1d8dd19",
    "vpc_id": "cef5d621-6c20-d5df-74e8-746271fba734",
    "ip_version": 4,
    "cidr": "192.168.21.96/28",
    "name": "name-test-updated",
    "description": "description-test-updated",
    "project_id": "11e8dd119c77479db890e266e68c1ecf",
    "created_at": "2024-09-09T11:56:27Z",
    "updated_at": "2024-09-09T12:00:06Z"
  },
  "request_id": "5e8c57bcfa0bd4798915cb5d7a37c1d9"
}
```

Status Codes

Status Code	Description
200	The PUT operation is successful. For more status codes, see Status Codes .

Error Codes

See [Error Codes](#).

5.12.5 Deleting a Subnet CIDR Reservation

Function

This API is used to delete a subnet CIDR reservation.

Calling Method

For details, see [Calling APIs](#).

URI

```
DELETE /v3/{project_id}/vpc/virsubnet-cidr-reservations/
{virsubnet_cidr_reservation_id}
```

Table 5-357 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see Obtaining a Project ID .
virsubnet_cidr_reservation_id	Yes	String	ID of a subnet CIDR reservation.

Request Parameters

None

Response Parameters

Status code: 204

The DELETE operation is successful. For more status codes, see [Status Codes](#).

None

Example Requests

Delete a single subnet CIDR reservation.

```
DELETE https://{Endpoint}/v3/{project_id}/vpc/virsubnet-cidr-reservations/ed4edb94-754c-7848-bb77-2d381906c535
```

Example Responses

None

Status Codes

Status Code	Description
204	The DELETE operation is successful. For more status codes, see Status Codes .

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 of the list request 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 ports accessible to the tenant submitting the request. A maximum of 2,000 records can be returned for each query operation. If the number of records exceeds 2,000, the pagination marker will be returned.

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_ad
dress={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	Mandat ory	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 <i>{ip_address}</i> to an IP address, for example, 192.168.21.22 or 2a07:b980:4030:14::1. Set <i>{subnet_id}</i> 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, 11th to 2,000th resource records will be returned. The default value of limit is 2000.
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 a set of zero or more allowed address pairs. This is an extended attribute. For details, see Table 6-11. - Instructions: - 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. - 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 network interface 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: <code>{"internal_elb": true}</code> – 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: <code>{"disable_security_groups": true }</code> 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: <pre>{"tcp_srvports": "port1 port2 port3", "udp_srvports": "port1 port2 port3"}</pre> 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: <pre>{"tcp_srvports": "80 443", "udp_srvports": "53"}</pre> 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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	- Specifies the time (UTC) when the port is updated. - Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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 network interface 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_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?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 a set of zero or more allowed address pairs. This is an extended attribute. For details, see Table 6-20. - Instructions: - 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. - 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 network interface 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 6-21 .
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: <code>{"internal_elb": true}</code> – 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: <code>{"disable_security_groups": true }</code> 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: <pre>{"tcp_srvports": "port1 port2 port3", "udp_srvports": "port1 port2 port3"}</pre> 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: <pre>{"tcp_srvports": "80 443", "udp_srvports": "53"}</pre> 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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	- Specifies the time (UTC) when the port is updated. - Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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 network interface 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 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	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_addresses_pairs	No	Array of allowed_addresses_pairs objects	Specifies a set of zero or more allowed address pairs. This is an extended attribute. For details, see Table 6-27. Instructions: • 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. • 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 network interface to 1.1.1.1/0.
extra_dhcp_options	No	Array of extra_dhcp_option 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: <code>{"internal_elb": true}</code> - 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: <code>{"disable_security_group s": true }</code> 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: <pre>{"tcp_srvports": "port1 port2 port3", "udp_srvports": "port1 port2 port3"}</pre> 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: <pre>{"tcp_srvports": "80 443", "udp_srvports": "53"}</pre> 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
<code>ip_address</code>	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 network interface to 1.1.1.1/0. - If the value of parameter allowed_address_pairs is specified, parameter ip_address is mandatory.
<code>mac_address</code>	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
<code>opt_name</code>	No	String	Specifies the option name.
<code>opt_value</code>	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 a set of zero or more allowed address pairs. This is an extended attribute. For details, see Table 6-32 . Instructions: • 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. • 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 network interface 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: <code>{"internal_elb": true}</code> – 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: <code>{"disable_security_groups": true }</code> 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: <pre>{"tcp_srvports": "port1 port2 port3", "udp_srvports": "port1 port2 port3"}</pre> 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: <pre>{"tcp_srvports": "80 443", "udp_srvports": "53"}</pre> 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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the port is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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. 0.0.0.0/0 is not supported.
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 a set of zero or more allowed address pairs. This is an extended attribute. For details, see Table 6-39. Instructions: • 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. • 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 network interface 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: <code>{"internal_elb": true}</code> - 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: <code>{"disable_security_groups": true }</code> 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: <pre>{"tcp_srvports": "port1 port2 port3", "udp_srvports": "port1 port2 port3"}</pre> 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: <pre>{"tcp_srvports": "80 443", "udp_srvports": "53"}</pre> 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 network interface 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 a set of zero or more allowed address pairs. This is an extended attribute. For details, see Table 6-44. Instructions: • 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. • 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 network interface 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: <code>{"internal_elb": true}</code> – 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: <code>{"disable_security_groups": true }</code> 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: <pre>{"tcp_srvports": "port1 port2 port3", "udp_srvports": "port1 port2 port3"}</pre> 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: <pre>{"tcp_srvports": "80 443", "udp_srvports": "53"}</pre> 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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the port is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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. 0.0.0.0/0 is not supported.
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

Queries all networks accessible to the tenant submitting the request. A maximum of 2,000 records can be returned for each query operation. If the number of records exceeds 2,000, the pagination marker will be returned.

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 networks 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, 11th to 2,000th resource records will be returned. The default value of limit is 2000.
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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the network is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the network is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the network is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the network is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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

Queries all subnets accessible to the tenant submitting the request. A maximum of 2,000 records can be returned for each query operation. If the number of records exceeds 2,000, the pagination marker will be returned.

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}&gate  
way_ip={subnet_gateway}&tenant_id={tenant_id}&enable_dhcp={is_enable_dhcp}
```

Example of querying subnets 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, 11th to 2,000th resource records will be returned. The default value of limit is 2000.
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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the subnet is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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:ffff"
  }],
  "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:ffff" }] In IPv6 subnet 2001:db8:a583:9::/64, IP addresses 2001:db8:a583:9::1, 2001:db8:a583:9:ffff:ffff:ffff:ffff, 2001:db8:a583:9:ffff:ffff:ffff:ffff, 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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the subnet is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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. This parameter cannot be set if the value of ip_version is 6 .
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 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 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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the subnet is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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. 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 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:ffff"}] 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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the subnet is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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	Mandato ry	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 ERROR .
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, 11th to 2,000th resource records will be returned. The default value of limit is 2000.
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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the router is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the router is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the router is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the router is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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-a7c8-3ccd5b7e755",
  "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 2,000 records can be returned for each query operation. If the number of records exceeds 2,000, the pagination marker will be returned.

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_v
ersion}&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

Paramet er	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.
descriptio n	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, 11th to 2,000th resource records will be returned. The default value of limit is 2000.

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 2,000 records can be returned for each query operation. If the number of records exceeds 2,000, the pagination marker will be returned.
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, 11th to 2,000th resource records will be returned. The default value of limit is 2000.
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	Mandato ry	Type	Description
firewall_policy_i d	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 2,000 records can be returned for each query operation. If the number of records exceeds 2,000, the pagination marker will be returned.

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	Mandator y	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, 11th to 2,000th resource records will be returned. The default value of limit is 2000.

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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the resource is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the resource is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

Example Response

```
{  
  "firewall_group": {  
    "status": "ACTIVE",
```



```
{
  "public": false,
  "egress_firewall_policy_id": null,
  "name": "bobby_fw1",
  "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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the resource is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the resource is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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	Mandato ry	Type	Description
firewall_group_i d	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 2,000 records can be returned for each query operation. If the number of records exceeds 2,000, the pagination marker will be returned.

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, 11th to 2,000th resource records will be returned. The default value of limit is 2000.
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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the security group is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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.

Attribute	Type	Description
remote_address_group_id	String	- Specifies the remote IP address group ID. - The parameter 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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the security group rule is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the security group is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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.

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 parameter 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 .

Attribute	Type	Description
created_at	String	Specifies the time (UTC) when the security group rule is created. Format: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the security group rule is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the security group is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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.

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 parameter 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 .

Attribute	Type	Description
created_at	String	Specifies the time (UTC) when the security group rule is created. Format: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the security group rule is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the security group is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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.

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 parameter 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 .

Attribute	Type	Description
created_at	String	Specifies the time (UTC) when the security group rule is created. Format: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the security group rule is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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 2,000 records can be returned for each query operation. If the number of records exceeds 2,000, the pagination marker will be returned.

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_i
p_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.
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.

Parameter	Mandatory	Type	Description
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, 11th to 2,000th resource records will be returned. The default value of limit is 2000.

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/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.

Attribute	Type	Description
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 parameter 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 .

Attribute	Type	Description
created_at	String	Specifies the time (UTC) when the security group rule is created. Format: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the security group rule is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

Table 6-195 SecurityGroupRulesLink 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_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.
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.

Attribute	Type	Description
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 parameter 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: <i>yyyy-MM-ddTHH:mm:ss</i>
updated_at	String	Specifies the time (UTC) when the security group rule is updated. Format: <i>yyyy-MM-ddTHH:mm:ss</i>

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": "6fbc9263116a4b68818cf1edce16bc4f",
  "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 Adding a Security Group Rule

Function

This API is used to add a security group rule. By default, allow rules can be created. For details about how to create deny rules, see the description of parameter **action** in section "Adding a Security Group Rule" in the *Virtual Private Cloud API Reference (V3)*.

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.

Attribute	Mandatory	Type	Description
remote_group_id	No	String	- Specifies the peer ID of the belonged security group. - This parameter value 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 value 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.
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.)

Attribute	Mandatory	Type	Description
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 parameter 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.
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.)

Attribute	Type	Description
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 parameter 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", "114.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 [Creating an ECS](#).

- 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.

- Send **PUT** [https://VPC endpoint/v1/{project_id}/ports/{port_id}](#). Parameter **project_id** indicates the project ID.
- Add **X-Auth-Token** to the request header.
- Specify the following parameters in the request body:

```
{
  "port": {
    "security_groups": ["9c0f56be-a9ac-438c-8c57-fce62de19419", "16b6e77a-08fa-42c7-aa8b-106c048884e6"]
  }
}
```

- 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 [Creating an ECS](#).
- 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 [Creating an ECS](#).
- 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.

- Send **GET** https://VPC endpoint/v2.0/ports?device_id={ecs_id}&network_id={network_id}.
- Add **X-Auth-Token** to the request header.
- 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 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 required permissions are determined by the actions supported by the API. Only users with the policies allowing for those 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 in a custom policy
- 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 Permissions and Supported Actions of API V1 and V2

8.2.1 VPC

Permission	API	Action
Creating a VPC	POST /v1/{project_id}/vpcs	vpc:vpcs:create
Querying a VPC	GET /v1/{project_id}/vpcs/{vpc_id}	vpc:vpcs:get
Querying VPCs	GET /v1/{project_id}/vpcs	vpc:vpcs:list
Updating a VPC	PUT /v1/{project_id}/vpcs/{vpc_id}	vpc:vpcs:update
Deleting a VPC	DELETE /v1/{project_id}/vpcs/{vpc_id}	vpc:vpcs:delete

8.2.2 Subnet

Permission	API	Action
Creating a subnet	POST /v1/{project_id}/subnets	vpc:subnets:create
Querying a subnet	GET /v1/{project_id}/subnets/{subnet_id}	vpc:subnets:get
Querying subnets	GET /v1/{project_id}/subnets	vpc:subnets:get
Updating a subnet	PUT /v1/{project_id}/vpcs/{vpc_id}/subnets/{subnet_id}	vpc:subnets:update
Deleting a subnet	DELETE /v1/{project_id}/vpcs/{vpc_id}/subnets/{subnet_id}	vpc:subnets:delete

8.2.3 Port

Permission	API	Action
Querying a port	GET /v1/{project_id}/ports	vpc:ports:get
Querying the details of a port	GET /v1/{project_id}/ports/{port_id}	vpc:ports:get
Updating a port	PUT /v1/{project_id}/ports/{port_id}	vpc:ports:update
Deleting a port	DELETE /v1/{project_id}/ports/{port_id}	vpc:ports:delete
Creating a port	POST /v1/{project_id}/ports	vpc:ports:create

8.2.4 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

8.2.5 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

8.2.6 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

8.2.7 Quota

Permission	API	Action
Querying quotas	GET /v1/{project_id}/quotas	vpc:quotas:list

8.2.8 Private IP Address

Permission	API	Action
Assigning a private IP address	POST /v1/{project_id}/privateips	vpc:privateips:create
Querying a private IP address	GET /v1/{project_id}/privateips/{privateip_id}	vpc:privateips:get
Querying private IP addresses	GET /v1/{project_id}/subnets/{subnet_id}/privateips	vpc:privateips:list
Releasing a private IP address	DELETE /v1/{project_id}/privateips/{privateip_id}	vpc:privateips:delete

8.2.9 Security Group

Permission	API	Action
Creating a security group	POST /v1/{project_id}/security-groups	vpc:securityGroups:create
Querying a security group	GET /v1/{project_id}/security-groups/{security_group_id}	vpc:securityGroups:get
Querying security groups	GET /v1/{project_id}/security-groups	vpc:securityGroups:get
Deleting a security group	DELETE /v1/{project_id}/security-groups/{security_group_id}	vpc:securityGroups:delete

8.2.10 Security Group Rule

Permission	API	Action
Adding a security group rule	POST /v1/{project_id}/security-group-rules	vpc:securityGroupRules:create
Querying a security group rule	GET /v1/{project_id}/security-group-rules/{rules_security_groups_id}	vpc:securityGroupRules:get
Querying security group rules	GET /v1/{project_id}/security-group-rules	vpc:securityGroupRules:get
Deleting a security group rule	DELETE /v1/{project_id}/security-group-rules/{rules_security_groups_id}	vpc:securityGroupRules:delete
Updating a security group rule	-	vpc:securityGroupRules:update

8.2.11 VPC Tag

Permission	API	Action
Adding a tag to a VPC	POST /v2.0/{project_id}/vpcs/{vpc_id}/tags	vpc:vpcTags:create
Querying tags of a VPC	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 adding 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 project	GET /v2.0/{project_id}/vpcs/tags	vpc:vpcTags:get

8.2.12 Subnet Tag

Permission	API	Action
Adding a tag to a subnet	POST /v2.0/{project_id}/subnets/{subnet_id}/tags	vpc:subnetTags:create
Querying tags of a subnet	GET /v2.0/{project_id}/subnets/{subnet_id}/tags	vpc:subnetTags:get
Deleting a tag from a subnet	DELETE /v2.0/{project_id}/subnets/{subnet_id}/tags/{key}	vpc:subnetTags:delete
Batch adding 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

8.2.13 VPC Flow Log

Permission	API	Action
Creating a flow log	POST /v1/{project_id}/fl/flow_logs	vpc:flowLogs:create
Querying flow logs	GET /v1/{project_id}/fl/flow_logs	vpc:flowLogs:get
Querying a flow log	GET /v1/{project_id}/fl/flow_logs/{flowlog_id}	vpc:flowLogs:get
Updating a 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

8.3 Permissions and Supported Actions of Native OpenStack Neutron V2.0

8.3.1 Port (OpenStack Neutron API)

Permission	API	Action
Querying ports	GET /v2.0/ports	vpc:ports:get
Querying a port	GET /v2.0/ports/{port_id}	vpc:ports:get
Creating a port	POST /v2.0/ports	vpc:ports:create
Updating a port	PUT /v2.0/ports/{port_id}	vpc:ports:update
Deleting a port	DELETE /v2.0/ports/{port_id}	vpc:ports:delete

8.3.2 Network (OpenStack Neutron API)

Permission	API	Action
Querying networks	GET /v2.0/networks	vpc:networks:get
Querying a network	GET /v2.0/networks/{network_id}	vpc:networks:get
Creating a network	POST /v2.0/networks	vpc:networks:create
Updating a network	PUT /v2.0/networks/{network_id}	vpc:networks:update
Deleting a network	DELETE /v2.0/networks/{network_id}	vpc:networks:delete

8.3.3 Subnet (OpenStack Neutron API)

Permission	API	Action
Querying subnets	GET /v2.0/subnets	vpc:subnets:get
Querying a subnet	GET /v2.0/subnets/{subnet_id}	vpc:subnets:get
Creating a subnet	POST /v2.0/subnets	vpc:subnets:create

Permission	API	Action
Updating a subnet	PUT /v2.0/subnets/{subnet_id}	vpc:subnets:update
Deleting a subnet	DELETE /v2.0/subnets/{subnet_id}	vpc:subnets:delete

8.3.4 Router (OpenStack Neutron API)

Permission	API	Action
Querying routers	GET /v2.0/routers	vpc:routers:get
Querying a router	GET /v2.0/routers/{router_id}	vpc:routers:get
Creating a router	POST /v2.0/routers	vpc:routers:create
Updating a router	PUT /v2.0/routers/{router_id}	vpc:routers:update
Deleting a router	DELETE /v2.0/routers/{router_id}	vpc:routers:delete
Adding an interface to a router	PUT /v2.0/routers/{router_id}/add_router_interface	- vpc:routers:addInterface - vpc:routers:get
Removing an interface from a router	PUT /v2.0/routers/{router_id}/remove_router_interface	- vpc:routers:removeInterface - vpc:routers:get

8.3.5 Network ACL (OpenStack Neutron API)

Permission	API	Action
Querying all network ACL rules	GET /v2.0/fwaas/firewall_rules	vpc:firewallRules:get
Querying a network ACL rule	GET /v2.0/fwaas/firewall_rules/{firewall_rule_id}	vpc:firewallRules:get

Permission	API	Action
Creating a network ACL rule	POST /v2.0/fwaas/firewall_rules	vpc:firewallRules:create
Updating a network ACL rule	PUT /v2.0/fwaas/firewall_rules/{firewall_rule_id}	vpc:firewallRules:update
Deleting a network ACL rule	DELETE /v2.0/fwaas/firewall_rules/{firewall_rule_id}	vpc:firewallRules:delete
Querying all network ACL policies	GET /v2.0/fwaas/firewall_policies	vpc:firewallPolicies:get
Querying a network ACL policy	GET /v2.0/fwaas/firewall_policies/{firewall_policy_id}	vpc:firewallPolicies:get
Creating a network ACL policy	POST /v2.0/fwaas/firewall_policies	vpc:firewallPolicies:create
Updating a network ACL policy	PUT /v2.0/fwaas/firewall_policies/{firewall_policy_id}	vpc:firewallPolicies:update
Deleting a network ACL policy	DELETE /v2.0/fwaas/firewall_policies/{firewall_policy_id}	vpc:firewallPolicies:delete
Inserting a network ACL rule	PUT /v2.0/fwaas/firewall_policies/{firewall_policy_id}/insert_rule	• vpc:firewallPolicies:addRule • vpc:firewallPolicies:get
Removing a network ACL rule	PUT /v2.0/fwaas/firewall_policies/{firewall_policy_id}/remove_rule	• vpc:firewallPolicies:removeRule • vpc:firewallPolicies:get
Querying all network ACL groups	GET /v2.0/fwaas/firewall_groups	vpc:firewallGroups:get
Querying a network ACL group	GET /v2.0/fwaas/firewall_groups/{firewall_group_id}	vpc:firewallGroups:get
Creating a network ACL group	POST /v2.0/fwaas/firewall_groups	vpc:firewallGroups:create

Permission	API	Action
Updating a network ACL group	PUT /v2.0/fwaas/firewall_groups/{firewall_group_id}	vpc:firewallGroups:update
Deleting a network ACL group	DELETE /v2.0/fwaas/firewall_groups/{firewall_group_id}	vpc:firewallGroups:delete

8.3.6 Security Group (OpenStack Neutron API)

Permission	API	Action
Querying a security group	GET /v2.0/security-groups	vpc:securityGroups:get
Querying the details of a security group	GET /v2.0/security-groups/{security_group_id}	vpc:securityGroups:get
Creating a security group	POST /v2.0/security-groups	vpc:securityGroups:create
Updating a security group	PUT /v2.0/security-groups/{security_group_id}	vpc:securityGroups:update
Deleting a security group	DELETE /v2.0/security-groups/{security_group_id}	vpc:securityGroups:delete
Querying a security group rule	GET /v2.0/security-group-rules	vpc:securityGroupRules:get
Querying the details of a security group rule	GET /v2.0/security-group-rules/{rules_security_groups_id}	vpc:securityGroupRules:get
Adding a security group rule	POST /v2.0/security-group-rules	vpc:securityGroupRules:create
Deleting a security group rule	DELETE /v2.0/security-group-rules/{rules_security_groups_id}	vpc:securityGroupRules:delete

8.4 Permissions and Supported Actions of API V3

8.4.1 VPC (V3)

Permission	API	Action
Querying VPC details	GET /v3/{project_id}/vpc/vpcs/{vpc_id}	vpc:vpcs:get
Querying VPCs	GET /v3/{project_id}/vpc/vpcs	vpc:vpcs:list
Adding a secondary CIDR block to a VPC	PUT /v3/{project_id}/vpc/vpcs/{vpc_id}/add-extend-cidr	vpc:vpcs:update
Removing a secondary CIDR block from a VPC	PUT /v3/{project_id}/vpc/vpcs/{vpc_id}/remove-extend-cidr	vpc:vpcs:update

8.4.2 Security Group (V3)

Permission	API	Action
Creating a security group	POST /v3/{project_id}/vpc/security-groups	vpc:securityGroups:create
Querying a security group	GET /v3/{project_id}/vpc/security-groups/{security_group_id}	vpc:securityGroups:get
Querying security groups	GET /v3/{project_id}/vpc/security-groups	vpc:securityGroups:get
Updating a security group	PUT /v3/{project_id}/vpc/security-groups/{security_group_id}	vpc:securityGroups:update
Deleting a security group	DELETE /v3/{project_id}/vpc/security-groups/{security_group_id}	vpc:securityGroups:delete

8.4.3 Security Group Rule (V3)

Permission	API	Action
Adding a security group rule	POST /v3/{project_id}/vpc/security-group-rules	vpc:securityGroupRules:create
Querying a security group rule	GET /v3/{project_id}/vpc/security-group-rules/{rules_security_groups_id}	vpc:securityGroupRules:get
Querying security group rules	GET /v3/{project_id}/vpc/security-group-rules	vpc:securityGroupRules:get
Deleting a security group rule	DELETE /v3/{project_id}/vpc/security-group-rules/{rules_security_groups_id}	vpc:securityGroupRules:delete
Updating a security group rule	-	vpc:securityGroupRules:update

8.4.4 IP Address Group (V3)

Permission	API	Action
Creating an IP address group	POST /v3/{project_id}/vpc/address-groups	vpc:addressGroups:create
Querying IP address groups	GET /v3/{project_id}/vpc/address-groups	vpc:addressGroups:list
Querying an IP address group	GET /v3/{project_id}/vpc/address-groups/{address_group_id}	vpc:addressGroups:get
Updating an IP address group	PUT /v3/{project_id}/vpc/address-groups/{address_group_id}	vpc:addressGroups:update
Deleting an IP address group	DELETE /v3/{project_id}/vpc/address-groups/{address_group_id}	vpc:addressGroups:delete
Forcibly deleting an IP address group	DELETE /v3/{project_id}/vpc/address-groups/{address_group_id}/force	vpc:addressGroups:delete

8.4.5 Supplementary Network Interface (V3)

Permission	API	Action
Creating a supplementary network interface	POST /v3/{project_id}/vpc/sub-network-interfaces	vpc:subNetworkInterfaces:create
Creating supplementary network interfaces in batches	POST /v3/{project_id}/vpc/sub-network-interfaces/batch-create	vpc:subNetworkInterfaces:create
Querying supplementary network interfaces	GET /v3/{project_id}/vpc/sub-network-interfaces	vpc:subNetworkInterfaces:list
Querying the details of a supplementary network interface	GET /v3/{project_id}/vpc/sub-network-interfaces/{sub_network_interface_id}	vpc:subNetworkInterfaces:get
Querying the number of supplementary network interfaces	GET /v3/{project_id}/vpc/sub-network-interfaces/count	vpc:subNetworkInterfaces:list
Updating a supplementary network interface	PUT /v3/{project_id}/vpc/sub-network-interfaces/{sub_network_interface_id}	vpc:subNetworkInterfaces:update
Deleting a supplementary network interface	DELETE /v3/{project_id}/vpc/sub-network-interfaces/{sub_network_interface_id}	vpc:subNetworkInterfaces:delete

8.4.6 Mirror Session (V3)

Permission	API	Action
Querying mirror sessions	GET /v3/{project_id}/vpc/traffic-mirror-sessions	vpc:trafficMirrorSessions:list

Permission	API	Action
Querying the details of a mirror session	GET /v3/{project_id}/vpc/traffic-mirror-sessions/{traffic_mirror_session_id}	vpc:trafficMirrorSessions:get
Creating a mirror session	POST /v3/{project_id}/vpc/traffic-mirror-sessions	vpc:trafficMirrorSessions:create
Updating a mirror session	PUT /v3/{project_id}/vpc/traffic-mirror-sessions/{traffic_mirror_session_id}	vpc:trafficMirrorSessions:update
Deleting a mirror session	DELETE /v3/{project_id}/vpc/traffic-mirror-sessions/{traffic_mirror_session_id}	vpc:trafficMirrorSessions:delete
Disassociating a mirror source from a mirror session	PUT /v3/{project_id}/vpc/traffic-mirror-sessions/{traffic_mirror_session_id}/remove-sources	vpc:trafficMirrorSessions:removeSource
Associating a mirror source with a mirror session	PUT /v3/{project_id}/vpc/traffic-mirror-sessions/{traffic_mirror_session_id}/add-sources	vpc:trafficMirrorSessions:addSource

8.4.7 Mirror Filter (V3)

Permission	API	Action
Creating a mirror filter	POST /v3/{project_id}/vpc/traffic-mirror-filters	vpc:trafficMirrorFilters:create
Querying mirror filters	GET /v3/{project_id}/vpc/traffic-mirror-filters	vpc:trafficMirrorFilters:list
Querying the details of a mirror filter	GET /v3/{project_id}/vpc/traffic-mirror-filters/{traffic_mirror_filter_id}	vpc:trafficMirrorFilters:get
Updating a mirror filter	PUT /v3/{project_id}/vpc/traffic-mirror-filters/{traffic_mirror_filter_id}	vpc:trafficMirrorFilters:update

Permission	API	Action
Deleting a mirror filter	DELETE /v3/{project_id}/vpc/traffic-mirror-filters/{traffic_mirror_filter_id}	vpc:trafficMirrorFilters:delete

8.4.8 Mirror Filter Rule (V3)

Permission	API	Action
Querying mirror filter rules	GET /v3/{project_id}/vpc/traffic-mirror-filter-rules	vpc:trafficMirrorFilterRules:list
Querying the details of a mirror filter rule	GET /v3/{project_id}/vpc/traffic-mirror-filter-rules/{traffic_mirror_filter_rule_id}	vpc:trafficMirrorFilterRules:get
Creating a mirror filter rule	POST /v3/{project_id}/vpc/traffic-mirror-filter-rules	vpc:trafficMirrorFilterRules:create
Updating a mirror filter rule	PUT /v3/{project_id}/vpc/traffic-mirror-filter-rules/{traffic_mirror_filter_rule_id}	vpc:trafficMirrorFilterRules:update
Deleting a mirror filter rule	DELETE /v3/{project_id}/vpc/traffic-mirror-filter-rules/{traffic_mirror_filter_rule_id}	vpc:trafficMirrorFilterRules:delete

8.4.9 Network ACL (V3)

Permission	API	Action
Creating a network ACL	POST /v3/{project_id}/vpc/firewalls	vpc:firewalls:create
Querying network ACLs	GET /v3/{project_id}/vpc/firewalls	vpc:firewalls:list
Querying the details of a network ACL	GET /v3/{project_id}/vpc/firewalls/{firewall_id}	vpc:firewalls:get

Permission	API	Action
Updating a network ACL	PUT /v3/{project_id}/vpc/firewalls/{firewall_id}	vpc:firewalls:update
Deleting a network ACL	DELETE /v3/{project_id}/vpc/firewalls/{firewall_id}	vpc:firewalls:delete
Updating a network ACL rule	PUT /v3/{project_id}/vpc/firewalls/{firewall_id}/update-rules	vpc:firewalls:update
Inserting a network ACL rule	PUT /v3/{project_id}/vpc/firewalls/{firewall_id}/insert-rules	vpc:firewalls:update
Deleting a network ACL rule	PUT /v3/{project_id}/vpc/firewalls/{firewall_id}/remove-rules	vpc:firewalls:update
Associating a subnet with a network ACL	PUT /v3/{project_id}/vpc/firewalls/{firewall_id}/associate-subnets	vpc:firewalls:update
Disassociating a subnet from a network ACL	PUT /v3/{project_id}/vpc/firewalls/{firewall_id}/disassociate-subnets	vpc:firewalls:update

8.4.10 Network ACL Tag (V3)

Permission	API	Action
Querying the number of network ACLs by tag	POST /v3/{project_id}/firewalls/resource-instances/count	vpc:firewallTags:get
Querying network ACLs by tag	POST /v3/{project_id}/firewalls/resource-instances/filter	vpc:firewallTags:get
Adding a tag to a network ACL	POST /v3/{project_id}/firewalls/{firewall_id}/tags	vpc:firewallTags:create

Permission	API	Action
Deleting a tag from a network ACL	DELETE /v3/{project_id}/firewalls/{firewall_id}/tags/{tag_key}	vpc:firewallTags:delete
Querying tags of a network ACL	GET /v3/{project_id}/firewalls/{firewall_id}/tags	vpc:firewallTags:get
Adding tags to a network ACL	POST /v3/{project_id}/firewalls/{firewall_id}/tags/create	vpc:firewallTags:create
Deleting tags from a network ACL	POST /v3/{project_id}/firewalls/{firewall_id}/tags/delete	vpc:firewallTags:delete
Querying tags of network ACLs in a project	GET /v3/{project_id}/firewalls/tags	vpc:firewallTags:get

8.4.11 Port (V3)

Permission	API	Action
Adding a security group to the security group list of a port	PUT /v3/{project_id}/ports/{port_id}/insert-security-groups	vpc:ports:update
Removing a security group from the security group list of a port	PUT /v3/{project_id}/ports/{port_id}/remove-security-groups	vpc:ports:update

8.5 Precautions for API Permissions

Note:

If you have insufficient permissions, response code **200** will be returned when you query network resources and an empty list will be displayed.

You can apply for the permissions and try again.

9 FAQs

9.1 What Are the Differences Between the VPC Subnet API and the OpenStack Neutron Subnet API?

Differences

Subnet APIs are classified into [VPC subnet APIs](#) and [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

Subnet Name	subnet-653b 	AZ	AZ3
Network ID	e06cc6c0-6967-4e0c-af03-7be3b5546ddd	Status	Normal
Subnet ID	97a14c19-fba4-46e3-9aab-60fae092aff7	DHCP	Enabled
CIDR Block	192.168.0.0/24	DNS Server Address	100.125.1.250,100.125.21.250  Reset
Gateway	192.168.0.1		

- The subnet ID used when calling the VPC subnet API is the network ID shown in [Figure 9-1](#). For example, e06cc6c0-6967-4e0c-af03-7be3b5546ddd.
- The subnet ID used when calling the OpenStack Neutron subnet API is the subnet ID shown in [Figure 9-1](#). For example, 97a14c19-fba4-46e3-9aab-60fae092aff7.

Example

The following queries subnet details to compare the difference.

VPC subnet API

```
GET /v1/049d06b7f20037e12f0dc0137381822f/subnets/e06cc6c0-6967-4e0c-af03-7be3b5546ddd
{
  "subnet": {
    "id": "e06cc6c0-6967-4e0c-af03-7be3b5546ddd", //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": "e06cc6c0-6967-4e0c-af03-7be3b5546ddd", //Correspond to the network ID
on the management console.
    "neutron_subnet_id": "97a14c19-fba4-46e3-9aab-60fae092aff7", //Correspond to the subnet ID on
the management console.
    "extra_dhcp_opts": []
  }
}
```

OpenStack Neutron subnet API

```
GET /v2.0/subnets/97a14c19-fba4-46e3-9aab-60fae092aff7
{
  "subnet": {
    "name": "subnet-54eb",
    "cidr": "192.168.0.0/24",
    "id": "97a14c19-fba4-46e3-9aab-60fae092aff7", //Correspond to the subnet ID on the management
console.
    "enable_dhcp": true,
    "network_id": "e06cc6c0-6967-4e0c-af03-7be3b5546ddd", //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?

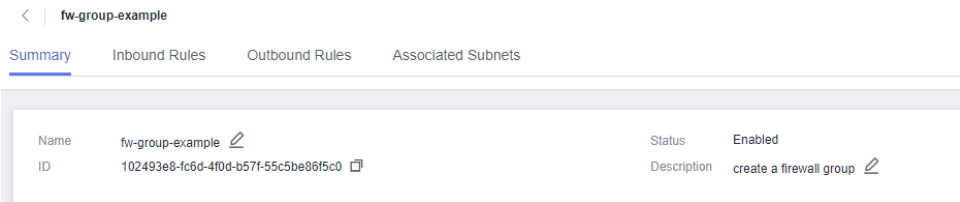
Relationships

Network ACL resources are classified into groups, policies, and rules.

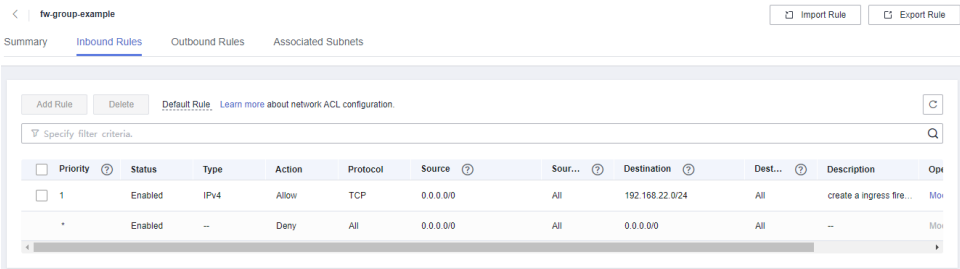
The relationships among them are as follows:

- 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.

< | fw-group-example

Summary

Inbound Rules

Outbound Rules

Associated Subnets

Name	fw-group-example 	Status	Enabled
ID	102493e8-fc6d-4f0d-b57f-55c5be86f5c0 	Description	create a firewall group 

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 allowed_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 allowed_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_pairs 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: <code>{"internal_elb": true}</code> • 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: <code>{"disable_security_groups": true },</code> 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 <code>"fixed_ips": [{"subnet_id": "4dc70db6-cb7f-4200-9790-a6a910776bba", "ip_address": "192.169.25.79"}]</code>. 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: <pre>{"internal_elb": true}</pre> • 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: <pre>{"disable_security_groups": true },</pre> 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_ad
dress={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, 11th to 2,000th resource records will be returned. The default value of limit is 2000.
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 <code>"fixed_ips": [{"subnet_id": "4dc70db6-cb7f-4200-9790-a6a910776bba", "ip_address": "192.169.25.79"}]</code>. 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: <pre>{"internal_elb": true}</pre> • 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: <pre>{"disable_security_groups": true },</pre> 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 allowed_address_pairs 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 allowed_address_pairs 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_opts 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_pairs 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: <code>{"internal_elb": true}</code> • 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: <code>{"disable_security_groups": true },</code> 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	Unit	Conversion Rule	Monitored Object (Dimension)	Monitoring Interval (Raw Data)
upstream_bandwidth	Outbound Bandwidth	Network rate of outbound traffic (Previously called "Upstream Bandwidth")	≥ 0	bit/s	1000 (SI)	Bandwidth or EIP	1 minute
downstream_bandwidth	Inbound Bandwidth	Network rate of inbound traffic (Previously called "Downstream Bandwidth")	≥ 0	bit/s	1000 (SI)	Bandwidth or EIP	1 minute

ID	Name	Description	Value Range	Unit	Conversion Rule	Monitored Object (Dimension)	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	0-100	%	N/A	Bandwidth or EIP	1 minute
upstream	Outbound Traffic	Network traffic going out of the cloud platform in a minute (Previously called "Upstream Traffic")	≥ 0	Byte	1000 (SI)	Bandwidth or EIP	1 minute
downstream	Inbound Traffic	Network traffic going into the cloud platform in a minute (Previously called "Downstream Traffic")	≥ 0	Byte	1000 (SI)	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.
202	Accepted	Specifies the normal response to the pre-check request of the V3 API.
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	EnterpriseProjectId 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 vpclId 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 it 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 Addresses	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 Addresses	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	privatelp 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 routetable 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 resourceInstances Req 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 resourceInstances Req 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 resourceInstances Req is invalid. Offset in resourceInstances Req is invalid.	Invalid limit or offset value.	Use valid limit and offset values.
	400	VPC.1801	ResourceInstances Req 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, resource 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.

Module	Status Code	Error Code	Message	Description	Handling Measure
Querying a VPC (V3)	404	VPC.9904	Vpc xxx could not be found.	The queried VPC does not exist.	Check whether the VPC to be queried exists.
Adding a secondary CIDR block to a VPC (V3)	400	VPC.9911	xxx is not a valid cidr format.	Invalid CIDR block format.	Enter a valid CIDR block.
	400	VPC.9912	Input extend cidr num xxx over limit xxx.	The number of secondary CIDR blocks to be added exceeds the upper limit.	Check whether there are too many secondary CIDR blocks in the VPC.
	409	VPC.9914	Add Extend cidr xxx conflict with exist cidr xxx.	The secondary CIDR block conflicts with an existing CIDR block.	Enter a different secondary CIDR block.
	400	VPC.9916	Add Extend cidr %s conflict with black list cidr %s-24.	The secondary CIDR block overlaps with a blacklisted CIDR block.	Enter a secondary CIDR block that is not blacklisted. For details about the secondary CIDR block blacklist, see the <i>API Reference</i> .
Removing a secondary CIDR block from a VPC (V3)	404	VPC.9915	Extend cidr xxx could not be found.	The secondary CIDR block to be removed does not exist.	Enter an existing secondary CIDR block.

Module	Status Code	Error Code	Message	Description	Handling Measure
Querying an IP address group	404	VPC.9904	Address_group xxx could not be found.	The IP address group does not exist.	Check whether the IP address group exists.
Creating an IP address group	400	VPC.9901	Duplicate ip_set in request body xxx.	The ip_set request body contains duplicate data.	Ensure that the ip_set request body does not contain duplicate data.
	400	VPC.9901	Invalid ip_set:xxx parameter in request body.	Invalid data in the value of parameter ip_set .	Ensure that the data in the value of parameter ip_set is valid.
	409	VPC.9905	Quota exceeded for resources: 'address_group'.	Insufficient IP address group quota.	Delete the address groups that are not required or increase the quota.
Updating an IP address group	400	VPC.9901	Duplicate ip_set in request body xxx.	The ip_set request body contains duplicate data.	Ensure that the ip_set request body does not contain duplicate data.
	400	VPC.9901	Invalid ip_set:xxx parameter in request body.	Invalid data in the value of parameter ip_set .	Ensure that the data in the value of parameter ip_set is valid.
	404	VPC.9904	Address_group xxx could not be found.	The IP address group to be updated does not exist.	Check whether the IP address group exists.

Module	Status Code	Error Code	Message	Description	Handling Measure
	409	VPC.9905	Quota exceeded for resources: ['address_group_contain_ipset'].	Insufficient IP address group rule quota.	Delete rules that are not required from the IP address group or increase the rule quota.
Deleting an IP address group	404	VPC.9904	Address_group xxx could not be found.	The IP address group to be deleted does not exist.	Check whether the IP address group exists.
	409	VPC.9907	1. Addressgroup xxx is used by securitygroup rules. 2. Addressgroup xxx is used by firewall rules.	1. The IP address group is used by a security group rule. 2. The IP address group is used by a network ACL rule.	Check whether the security group rule or network ACL rule is required. If not, use the API for forcibly deleting the IP address group.
Querying a security group (V3)	404	VPC.9904	Security group xxx does not exist.	The security group to be queried does not exist.	Check whether the security group to be queried exists.
Creating a security group (V3)	409	VPC.9905	Quota exceeded for resources: security_group.	Insufficient security group quota.	Delete the security groups that are not required or increase the quota.
Updating a security group (V3)	404	VPC.9904	SecurityGroup xxx could not be found.	The security group to be updated does not exist.	Check whether the security group to be queried exists.

Module	Status Code	Error Code	Message	Description	Handling Measure
Deleting a security group (V3)	404	VPC.9904	Security_group xxx could not be found.	The security group to be deleted does not exist.	Check whether the security group exists.
	409	VPC.9902	Security Group xxx is in use.	The security group to be deleted is associated with a port.	Disassociate the port from the security group and try again.
Querying a security group rule (V3)	404	VPC.9904	Security_group_rule xxx could not be found.	The security group rule to be queried does not exist.	Check whether the security group rule exists.
Creating a security group rule (V3)	409	VPC.9905	Quota exceeded for resources: ['security_group_rule'].	Insufficient security group rule quota.	Delete the security group rules that are not required or increase the quota.
	404	VPC.9904	security_group_id xxx could not be found.	The security group defined by security_group_id does not exist.	Check whether the security group information is correct.
	404	VPC.9904	remote security group xxx could not be found.	The security group defined by remote_group_id does not exist.	Check whether the security group information is correct.

Module	Status Code	Error Code	Message	Description	Handling Measure
	404	VPC.9904	Address group xxx does not exist.	The IP address group defined by remote_address_group_id does not exist.	Check whether the IP address group information is correct.
	400	VPC.9902	Security group rule for ethertype xxx not supported. Allowed values are [IPv4, IPv6].	Invalid ethertype value.	Modify the request parameter. Enter a valid ethertype value. Supported values are IPv4 and IPv6, which are case insensitive.
	400	VPC.9902	Ethertype xxx and address_group ip_version xxx not match	The ethertype value in the request is inconsistent with the IP version of the IP address group.	Check the IP version of the IP address group defined by remote_address_group_id . The IP address version must be the same as the ethertype value.
	409	VPC.9902	Security group rule already exists. Rule id is xxx.	The security group rule already exists.	Ensure that the specified security group rule does not conflict with existing rules.

Module	Status Code	Error Code	Message	Description	Handling Measure
Deleting a security group rule (V3)	404	VPC.9904	Security_group_rule xxx could not be found.	The security group rule to be queried does not exist.	Check whether the security group rule exists.

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

