Elastic Load Balance

API Reference

Issue 01

Date 2025-02-25

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Contents

1 Before You Start

Welcome to *Elastic Load Balance API Reference*. ELB distributes incoming traffic across backend servers based on the routing rules you define. ELB expands the service capabilities of applications and improves their availability by eliminating single points of failure (SPOFs).

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

If you plan to access load balancers and associated resources through an API, ensure that you are familiar with ELB concepts. For details, see **Service Overview**.

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

Additionally, ELB offers software development kits (SDKs) for multiple programming languages. For how to use SDKs, see **Huawei Cloud SDKs**.

Constraints

- The number of load balancers and associated resources that you can create are determined by your quotas. To view or increase the quota, see **What Is Quota?**
- For more constraints, see the description of each API.

Endpoints

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

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. To ensure

account security, 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**.

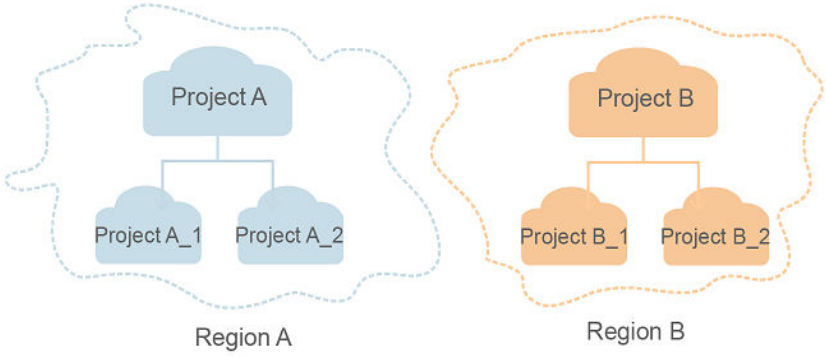
- AZ

  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***.

2 API Overview

A combination of these types of APIs allows you to use all functions provided by ELB. **Table 2-1** describes the APIs provided by ELB.

Table 2-1 ELB APIs

Type	Resource	Description
APIs (Dedicated load balancers)	Load balancer	Creates, updates, deletes a load balancer, shows the details of a load balancer, lists load balancers, and queries the status tree for a load balancer.
	Certificate	Creates, modifies, and deletes a certificate, and lists certificates.
	Security policy	Adds, modifies, and deletes a security policy, shows the details of a security policy, and lists security policies.
	IP address group	Configures, modifies, and disables an IP address group, shows the details of an IP address group, and lists IP address groups.
	Listener	Adds, modifies, and deletes a listener, shows the details of a listener, and lists listeners.
	Backend server group	Adds, modifies, and deletes a backend server group, shows the details of a backend server group, and lists backend server groups.
	Backend server	Adds, modifies, and deletes a backend server, shows the details of a backend server, and lists backend servers.
	Health check	Configures, modifies, and disables a health check, shows the details of a health check, and lists health checks.

Type	Resource	Description
	Forwarding policy	Adds, updates, and deletes a forwarding policy, shows the details of a forwarding policy, lists forwarding policies, and updates forwarding policy priorities.
	Forwarding rule	Adds, modifies, and deletes a forwarding rule, shows the details of a forwarding rule, and lists forwarding rules.
Shared load balancer APIs	Load balancer	Creates, updates, deletes a load balancer, shows the details of a load balancer, lists load balancers, and queries the status tree for a load balancer.
	Listener	Adds, updates, and deletes a listener, shows the details of a listener, and lists listeners.
	Backend server group	Adds, updates, and deletes a backend server group, shows the details of a backend server group, and lists backend server groups.
	Backend server	Adds, updates, and removes a backend server, shows the details of a backend server, and lists backend servers.
	Health check	Configures, updates, and disables a health check, and shows the details of a health check.
	Forwarding policy	Adds, updates, and deletes a forwarding policy, shows the details of a forwarding policy, and lists forwarding policies.
	Forwarding rule	Adds, updates, and deletes a forwarding rule, shows the details of a forwarding rule, and lists forwarding rules.
	Whitelist	Creates, updates, and deletes a certificate, and lists whitelist.
	SSL certificate	Creates, updates, and deletes a certificate, and lists certificates.
Shared load balancer APIs (OpenStack)	Load balancer	Creates, updates, deletes a load balancer, shows the details of a load balancer, lists load balancers, and queries the status tree for a load balancer.
	Listener	Adds, updates, and deletes a listener, shows the details of a listener, and lists listeners.
	Backend server group	Adds, updates, and deletes a backend server group, shows the details of a backend server group, and lists backend server groups.

Type	Resource	Description
	Backend server	Adds, updates, and removes a backend server, shows the details of a backend server, and lists backend servers.
	Health check	Configures, updates, and disables a health check, and shows the details of a health check.
	Forwarding policy	Adds, updates, and deletes a forwarding policy, shows the details of a forwarding policy, and lists forwarding policies.
	Forwarding rule	Adds, updates, and deletes a forwarding rule, shows the details of a forwarding rule, and lists forwarding rules.
	Whitelist	Creates, updates, and deletes a certificate, and lists whitelist.
	SSL certificate	Creates, updates, and deletes a certificate, and lists certificates.
	Tag	Adds a tag to and deletes a tag from a load balancer, batch adds and deletes load balancer tags, lists all tags of a load balancer, lists tags of all load balancers, queries load balancers by tag, adds and deletes a tag to a listener, batch adds and deletes tags to a listener, lists all tags of a listener, lists tags of all listeners, and queries listeners by tag.

3 Selecting an API Version

Elastic Load Balance (ELB) provides two versions of APIs: V2 and V3. For details about how to select an API version, see **Table 3-1**. For details about the overall APIs and their functions, see **API Overview**.

Table 3-1 ELB API versions

API Version	Description	Load Balancer Type
V3	• Can be used to perform all operations on dedicated load balancers. • Can be used to perform all operations on existing shared load balancers except for creating new ones.	Dedicated load balancers
V2	Can be used to perform all operations on shared load balancers.	Shared load balancers

4 Calling APIs

4.1 Making an API Request

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

Request URI

A request URI is in the following format:

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

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

Table 4-1 URI parameter description

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

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

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

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

Figure 4-1 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 4-2 HTTP methods

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

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

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

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

Request Header

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

Common request header fields are as follows.

Table 4-3 Common request header fields

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

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

NOTE

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

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

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

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

(Optional) Request Body

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

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

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

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

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

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

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

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

4.2 Authentication

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

- 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: Requests are authenticated using tokens.

AK/SK Authentication

NOTE

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

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

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

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

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

Token Authentication

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

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

IMS 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": $ADMIN_PASS,  //IAM user password. You are advised to store it in ciphertext in the configuration file or an environment variable and decrypt it when needed to ensure security.
                    "domain": {
                        "name": "domainname"  // Name of the account to which the IAM user belongs
                    }
                }
            }
        },
        "scope": {
            "project": {
                "name": "xxxxxxxx"    // Project name
            }
        }
    }
}
```

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

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3.0/OS-USER/users
Content-Type: application/json
X-Auth-Token: ABCDEFJ....
```

4.3 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 4-2 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 4-2 Header fields of the response to the request for creating an IAM user

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

(Optional) Response Body

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

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

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



```
    }
}
```

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

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

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

5 APIs (V3)

5.1 API Version

5.1.1 Querying API Versions

Function

This API is used to query all available ELB API versions.

Calling Method

For details, see **Calling APIs**.

URI

GET /versions

Request Parameters

None

Response Parameters

Status code: 200

Table 5-1 Response body parameters

Parameter	Type	Description
versions	Array of **ApiVersionInfo** objects	Lists the available API versions.

Table 5-2 ApiVersionInfo

Parameter	Type	Description
id	String	Specifies the API version. The value can be **v3**, **v2**, or **v2.0** in ascending order.
status	String	Specifies the status of the API version. The values are as follows: • **CURRENT**: current version • **STABLE**: stable version • **DEPRECATED**: discarded version Note: **CURRENT** indicates the latest version.

Example Requests

Querying API versions of a load balancer

```
GET https://{ELB_Endpoint}/versions
```

Example Responses

Status code: 200

Successful request.

```
{
  "versions" : [ {
    "id" : "v3",
    "status" : "CURRENT"
  }, {
    "id" : "v2",
    "status" : "STABLE"
  }, {
    "id" : "v2.0",
    "status" : "STABLE"
  } ]
}
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;
```



```
public class ListApiVersionsSolution {

    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");

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

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ListApiVersionsRequest request = new ListApiVersionsRequest();
        try {
            ListApiVersionsResponse response = client.listApiVersions(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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"]

    credentials = BasicCredentials(ak, sk)

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

    try:
        request = ListApiVersionsRequest()
        response = client.list_api_versions(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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")

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

    client := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListApiVersionsRequest{}
    response, err := client.ListApiVersions(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	Successful request.

Error Codes

See **Error Codes**.

5.2 Quota

5.2.1 Querying Quotas

Function

This API is used to query the quotas of load balancers and related resources in a specific project.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/quotas

Table 5-3 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Request Parameters

Table 5-4 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-5 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.

Parameter	Type	Description
quota	**Quota** object	Specifies the quotas of load balancers and associated resources. Only the total quotas are returned. Remaining available quotas will not be returned.

Table 5-6 Quota

Parameter	Type	Description
project_id	String	Specifies the project ID.
loadbalancer	Integer	Specifies the load balancer quota. • If the value is greater than or equal to 0, it indicates the load balancer quota. • If the value is **-1**, the quota is not limited.
certificate	Integer	Specifies the certificate quota. • If the value is greater than or equal to 0, it indicates the certificate quota. • If the value is **-1**, the quota is not limited.
listener	Integer	Specifies the listener quota. • If the value is greater than or equal to 0, it indicates the listener quota. • If the value is **-1**, the quota is not limited.
l7policy	Integer	Specifies the forwarding policy quota. • If the value is greater than or equal to 0, it indicates the forwarding policy quota. • If the value is **-1**, the quota is not limited.
condition_per_policy	Integer	Specifies the maximum number of forwarding rules per forwarding policy. • If the value is greater than or equal to 0, it indicates the current quota. • **-1** indicates that the quota is not limited.

Parameter	Type	Description
pool	Integer	Specifies the backend server group quota. • If the value is greater than or equal to 0, it indicates the backend server group quota. • If the value is **-1**, the quota is not limited.
healthmonitor	Integer	Specifies the health check quota. • If the value is greater than or equal to 0, it indicates the health check quota. • If the value is **-1**, the quota is not limited.
member	Integer	Specifies the backend server quota. • If the value is greater than or equal to 0, it indicates the backend server quota. • If the value is **-1**, the quota is not limited.
members_per_pool	Integer	Specifies the maximum number of backend servers in a backend server group. • If the value is greater than or equal to 0, it indicates the backend server quota. • If the value is **-1**, the quota is not limited.
listeners_per_pool	Integer	Specifies the maximum number of listeners that can be associated with a backend server group. • If the value is greater than or equal to 0, it indicates the current quota. • **-1** indicates that the quota is not limited.
ipgroup	Integer	Specifies the IP address group quota. • If the value is greater than or equal to 0, it indicates the IP address group quota. • If the value is **-1**, the quota is not limited.

Parameter	Type	Description
ipgroup_bindings	Integer	Specifies the maximum number of listeners that can be associated with an IP address group. • If the value is greater than or equal to 0, it indicates the maximum number of listeners that can be associated with an IP address group. • If the value is **-1**, the quota is not limited.
ipgroup_max_length	Integer	Specifies the maximum number of IP addresses that can be added to an IP address group. • If the value is greater than or equal to 0, it indicates the IP address quota. • If the value is **-1**, the quota is not limited.
security_policy	Integer	Specifies the custom security policy quota. • If the value is greater than or equal to 0, it indicates the custom security policy quota. • If the value is **-1**, the quota is not limited.
listeners_per_loadbalancer	Integer	Specifies the maximum number of listeners that can be associated with a load balancer. Value options: • If the value is greater than or equal to 0, it indicates the current quota. • **-1** indicates that the quota is not limited. Note: The maximum number of listeners that can be added to each load balancer is not limited, but it is recommended that the listeners not exceed the default quota.

Parameter	Type	Description
ipgroups_per_listener	Integer	Specifies the maximum number of IP address groups that can be associated with a listener. Value options: • If the value is greater than or equal to 0, it indicates the IP address group quota. • **-1** indicates that the quota is not limited.
pools_per_l7policy	Integer	Specifies the maximum number of backend server groups that can be used by a forwarding policy. Value options: • If the value is greater than or equal to 0, it indicates the backend server group quota. • **-1** indicates that the quota is not limited.
l7policies_per_listener	Integer	Specifies the maximum number of forwarding policies that can be configured for a listener. Value options: • If the value is greater than or equal to 0, it indicates the forwarding policy quota. • **-1** indicates that the quota is not limited.

Example Requests

Querying the quotas of resources associated with a load balancer.

```
GET https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/quotas
```

Example Responses

Status code: 200

Successful request.

```
{
  "request_id" : "c6f3d7fe99bb1d8aa29e148097dab0d0",
  "quota" : {
    "member" : 10000,
    "members_per_pool" : 1000,
    "certificate" : -1,
    "l7policy" : 2000,
    "listener" : 1500,
```



```
    "loadbalancer" : 100000,
    "healthmonitor" : -1,
    "pool" : 5000,
    "ipgroup" : 1000,
    "ipgroup_bindings" : 50,
    "ipgroup_max_length" : 300,
    "security_policy" : 50,
    "project_id" : "060576798a80d5762fafc01a9b5eedc7",
    "condition_per_policy" : 10,
    "listeners_per_pool" : 50,
    "listeners_per_loadbalancer" : 50
  }
}
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ShowQuotaSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowQuotaRequest request = new ShowQuotaRequest();
        try {
            ShowQuotaResponse response = client.showQuota(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowQuotaRequest()
        response = client.show_quota(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
```



```
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowQuotaRequest{}
    response, err := client.ShowQuota(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	Successful request.

Error Codes

See **Error Codes**.

5.2.2 Querying Quota Usage

Function

This API is used to query the current quotas and used quotas of resources related to a load balancer in a specific project.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/quotas/details

Table 5-7 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Table 5-8 Query Parameters

Parameter	Mandatory	Type	Description
quota_key	No	Array of strings	Specifies the resource type. The value can be **loadbalancer**, **listener**, **ipgroup**, **pool**, **member**, **healthmonitor**, **l7policy**, **certificate**, **security_policy**, **listeners_per_loadbalancer**, **listeners_per_pool**, **members_per_pool**, **condition_per_policy**, **ipgroup_bindings**, **ipgroup_max_length**, **ipgroups_per_listener**, **pools_per_l7policy**, or **l7policies_per_listener**. Multiple values can be queried in the format of *quota_key=xxx&quota_key=xxx*.

Request Parameters

Table 5-9 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-10 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
quotas	Array of **QuotaInfo** objects	Specifies the resource quotas.

Table 5-11 QuotaInfo

Parameter	Type	Description
quota_key	String	Specifies the resource type. The value can be **loadbalancer**, **listener**, **ipgroup**, **pool**, **member**, **healthmonitor**, **l7policy**, **certificate**, **security_policy**, **listeners_per_loadbalancer**, **listeners_per_pool**, **members_per_pool**, **condition_per_policy**, **ipgroup_bindings**, **ipgroup_max_length**, **ipgroups_per_listener**, **pools_per_l7policy**, or **l7policies_per_listener**.
quota_limit	Integer	Specifies the total quota. Value options: • If the value is greater than or equal to 0, it indicates the current quota. • **-1** indicates that the quota is not limited.
used	Integer	Specifies the used quota.
unit	String	Specifies the quota unit. The value can only be **count**.

Example Requests

Querying the quota of a specific ELB resource type

```
https://{ELB_Endpoint}/v3/06b9dc6cbf80d5952f18c0181a2f4654/elb/quotas/details?
quota_key=members_per_pool&quota_key=loadbalancer
```

Example Responses

Status code: 200

Successful request.

```
{
  "request_id" : "a396ad8e282d69d1afec6d437fe93c2d",
  "quotas" : [ {
    "quota_key" : "members_per_pool",
    "used" : 992,
    "quota_limit" : 1000,
    "unit" : "count"
  }, {
    "quota_key" : "security_policy",
    "used" : 11,
    "quota_limit" : 50,
    "unit" : "count"
```



```
}, {
  "quota_key" : "ipgroup_max_length",
  "used" : 3,
  "quota_limit" : 300,
  "unit" : "count"
}, {
  "quota_key" : "listener",
  "used" : 803,
  "quota_limit" : 1500,
  "unit" : "count"
}, {
  "quota_key" : "pool",
  "used" : 1009,
  "quota_limit" : 5000,
  "unit" : "count"
}, {
  "quota_key" : "certificate",
  "used" : 608,
  "quota_limit" : -1,
  "unit" : "count"
}, {
  "quota_key" : "loadbalancer",
  "used" : 752,
  "quota_limit" : 100000,
  "unit" : "count"
}, {
  "quota_key" : "ipgroup",
  "used" : 11,
  "quota_limit" : 1000,
  "unit" : "count"
}, {
  "quota_key" : "ipgroup_bindings",
  "used" : 2,
  "quota_limit" : 50,
  "unit" : "count"
}, {
  "quota_key" : "member",
  "used" : 3022,
  "quota_limit" : 10000,
  "unit" : "count"
}, {
  "quota_key" : "listeners_per_loadbalancer",
  "used" : 0,
  "quota_limit" : 50,
  "unit" : "count"
}, {
  "quota_key" : "l7policy",
  "used" : 148,
  "quota_limit" : 2000,
  "unit" : "count"
}, {
  "quota_key" : "healthmonitor",
  "used" : 762,
  "quota_limit" : -1,
  "unit" : "count"
}, {
  "quota_key" : "ipgroups_per_listener",
  "used" : 5,
  "quota_limit" : 10,
  "unit" : "count"
}, {
  "quota_key" : "pools_per_l7policy",
  "used" : 5,
  "quota_limit" : 100,
  "unit" : "count"
}, {
  "quota_key" : "l7policies_per_listener",
  "used" : 5,
  "quota_limit" : 100,
```



```
    "unit" : "count"
  } ]
}
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ListQuotaDetailsSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ListQuotaDetailsRequest request = new ListQuotaDetailsRequest();
        try {
            ListQuotaDetailsResponse response = client.listQuotaDetails(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListQuotaDetailsRequest()
        response = client.list_quota_details(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListQuotaDetailsRequest{}
    response, err := client.ListQuotaDetails(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	Successful request.

Error Codes

See **Error Codes**.

5.3 AZ

5.3.1 Querying AZs

Function

This API is used to query all available AZs when you create a load balancer.

Note the following when you create a load balancer:

- One set of AZs is returned by default. When you create a dedicated load balancer, you can select one or more AZs only in this set.
- If **loadbalancer_id** is specified, the set of AZs in the cluster where the load balancer resides is returned.
- In special scenarios, dedicated load balancers must be created in specific AZs. In the returned one or more sets of AZs, you can select as many AZs as you want as long as the selected AZs are in the same set. For example, if two sets **[az1,az2]** and **[az2,az3]** are returned, you can select **az1** and **az2** or **az2** and **az3**, but cannot select **az1** and **az3**.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/availability-zones

Table 5-12 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Table 5-13 Query Parameters

Parameter	Mandatory	Type	Description
public_border_group	No	String	Specifies the public border group.
loadbalancer_id	No	String	Specifies the load balancer ID.

Request Parameters

Table 5-14 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-15 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. The value is automatically generated.
availability_zones	Array<Array<**AvailabilityZone**>>	Specifies the AZs that are available during load balancer creation. For example, in **[az1,az2]** and **[az2,az3]** sets, you can select **az1** and **az2** or **az2** and **az3**, but cannot select **az1** and **az3**.
spec_code	String	Specifies the product specification code for the edge AZ.

Table 5-16 AvailabilityZone

Parameter	Type	Description
code	String	Specifies the AZ code.
state	String	Specifies the AZ status. The value can only be **ACTIVE**.
protocol	Array of strings	Specifies the type of the flavor that is not sold out. Value options: • **L4** indicates the flavor at Layer 4 (flavor for network load balancing). • **L7** indicates the flavor at Layer 7 (flavor for application load balancing).
public_border_group	String	Specifies the public border group, for example, **center**.
category	Integer	Specifies the AZ code. **0** indicates **center**. **21** indicates **homezone**.

Example Requests

Querying AZs where a load balancer works

```
GET https://{ELB_Endpoint}/v3/060576782980d5762f9ec014dd2f1148/elb/availability-zones
```

Example Responses

Status code: 200

Successful request.

```
{
  "availability_zones" : [ [ {
    "state" : "ACTIVE",
    "code" : "az1",
    "protocol" : [ "L4", "L7" ],
    "public_border_group" : "center",
    "category" : 0
  }, {
    "state" : "ACTIVE",
    "code" : "az2",
    "protocol" : [ "L4" ],
    "public_border_group" : "center",
    "category" : 0
  }, {
    "state" : "ACTIVE",
    "code" : "az3",
    "protocol" : [ "L7" ],
    "public_border_group" : "center",
    "category" : 0
  }, {
    "state" : "ACTIVE",
    "code" : "homezone.az0",
    "protocol" : [ "L4" ],
```



```
    "public_border_group" : "homezone.azg",
    "category" : 21
  } ] ],
  "request_id" : "0d799435-259e-459f-b2bc-0beee06f6a77"
}
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ListAvailabilityZonesSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ListAvailabilityZonesRequest request = new ListAvailabilityZonesRequest();
        try {
            ListAvailabilityZonesResponse response = client.listAvailabilityZones(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListAvailabilityZonesRequest()
        response = client.list_availability_zones(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListAvailabilityZonesRequest{}
    response, err := client.ListAvailabilityZones(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	Successful request.

Error Codes

See **Error Codes**.

5.4 Load Balancer Flavor

5.4.1 Querying Flavors

Function

This API is used to query all load balancer flavors that are available to a specific user in a specific region.

Constraints

This API has the following constraints:

- Parameters **marker**, **limit**, and **page_reverse** are used for pagination query.
- Parameters **marker** and **page_reverse** take effect only when they are used together with parameter **limit**.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/flavors

Table 5-17 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Table 5-18 Query Parameters

Parameter	Mandatory	Type	Description
marker	No	String	Specifies the ID of the last record on the previous page. Note: • This parameter must be used together with **limit**. • If this parameter is not specified, the first page will be queried. • This parameter cannot be left blank or set to an invalid ID.
limit	No	Integer	Specifies the number of records on each page. Value range: 0–2000 Default value: 2000
page_reverse	No	Boolean	Specifies whether to use reverse query. Value options: • **true**: Query the previous page. • **false** (default): Query the next page. Note: • This parameter must be used together with **limit**. • If **page_reverse** is set to **true** and you want to query the previous page, set the value of **marker** to the value of **previous_marker**.
id	No	Array of strings	Specifies the flavor ID. Multiple IDs can be queried in the format of *id=xxx&id=xxx*.

Parameter	Mandatory	Type	Description
name	No	Array of strings	Specifies the flavor name. Multiple names can be queried in the format of *name=xxx&name=xxx*.
type	No	Array of strings	Specifies the flavor type. Value options: • **L4** indicates a Layer 4 flavor. • **L7** indicates a Layer 7 flavor. • **L4_elastic** indicates the minimum elastic flavor at Layer 4. • **L7_elastic** indicates the minimum elastic flavor at Layer 7. • **L4_elastic_max** indicates the maximum elastic flavor at Layer 4. • **L7_elastic_max** indicates the maximum elastic flavor at Layer 7. Multiple types can be queried in the format of *type=xxx&type=xxx*.
shared	No	Boolean	Specifies whether the flavor is available to all users. • **true** indicates that the flavor is available to all users. • **false** indicates that the flavor is available only to a specific user.
public_border_group	No	Array of strings	Specifies the public border group. Multiple values can be queried in the format of *public_border_group=xxx&public_border_group=xxx*.
category	No	Array of integers	Specifies the category. Multiple values can be queried in the format of *category=xxx&category=xxx*.

Parameter	Mandatory	Type	Description
list_all	No	Boolean	If **list_all** is set to **true**, all maximum elastic specifications defined by **l4_elastic_max** and **l7_elastic_max** are returned. If **list_all** is set to **false**, only the largest elastic specifications will be returned. For Layer 4 load balancers, the specification with highest **cps** value is returned. If the **cps** values are the same, the specification with highest **bandwidth** value is returned. For Layer 7 load balancers, the specification with highest **https_cps** value is returned. If the **https_cps** values are the same, the specification with highest **qps** value is returned.
flavor_sold_out	No	Boolean	Specifies whether the flavor is available. • **true** indicates the flavor is unavailable. • **false** indicates the flavor is available.

Request Parameters

Table 5-19 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-20 Response body parameters

Parameter	Type	Description
flavors	Array of **Flavor** objects	Lists the flavors.
page_info	**PageInfo** object	Shows pagination information about the load balancer flavors.
request_id	String	Specifies the request ID. Note: The value is automatically generated.

Table 5-21 Flavor

Parameter	Type	Description
id	String	Specifies the flavor ID.
info	**FlavorInfo** object	Specifies the flavor metrics.
name	String	Specifies the flavor name. Network load balancers have the following flavors: • L4_flavor.elb.s1.small: small I • L4_flavor.elb.s2.small: small II • L4_flavor.elb.s1.medium: medium I • L4_flavor.elb.s2.medium: medium II • L4_flavor.elb.s1.large: large I • L4_flavor.elb.s2.large: large II • L4_flavor.elb.pro.max: elastic flavor at Layer 4 Application load balancers have the following flavors: • L7_flavor.elb.s1.small: small I • L7_flavor.elb.s2.small: small II • L7_flavor.elb.s1.medium: medium I • L7_flavor.elb.s2.medium: medium II • L7_flavor.elb.s1.large: large I • L7_flavor.elb.s2.large: large II • L7_flavor.elb.s1.extra-large: extra-large I • L7_flavor.elb.s2.extra-large: extra-large II • L7_flavor.elb.pro.max: elastic flavor at Layer 7

Parameter	Type	Description
shared	Boolean	Specifies whether the flavor is available to all users. • **true** indicates that the flavor is available to all users. • **false** indicates that the flavor is available only to a specific user.
project_id	String	Specifies the project ID.
type	String	Specifies the flavor type. The type can be: • **L4** indicates a Layer 4 flavor. • **L7** indicates a Layer 7 flavor. • **L4_elastic** indicates the minimum elastic flavor at Layer 4. This parameter has been discarded. Please do not use it. • **L7_elastic** indicates the minimum elastic flavor at Layer 7. This parameter has been discarded. Please do not use it. • **L4_elastic_max** indicates the maximum elastic flavor at Layer 4. • **L7_elastic_max** indicates the maximum elastic flavor at Layer 7.
flavor_sold_out	Boolean	Specifies whether the flavor is available. • **true** indicates the flavor is unavailable. • **false** indicates the flavor is available.
public_border_group	String	Specifies the public border group, for example, **center**.
category	Integer	Specifies the public border group code. **0** indicates **center**. **21** indicates **homezone**.

Table 5-22 FlavorInfo

Parameter	Type	Description
connection	Integer	Specifies the number of concurrent connections per second.

Parameter	Type	Description
cps	Integer	Specifies the number of new connections per second.
qps	Integer	Specifies the number of requests per second. This parameter is available only for load balancers at Layer 7.
bandwidth	Integer	Specifies the bandwidth, in kbit/s
lcu	Integer	Specifies the number of LCUs in the flavor. **NOTE** An LCU measures the dimensions on which a dedicated load balancer routes the traffic. The higher value indicates better performance.
https_cps	Integer	Specifies the number of new HTTPS connections. This parameter is available only for load balancers at Layer 7.

Table 5-23 PageInfo

Parameter	Type	Description
previous_marker	String	Specifies the ID of the first record in the pagination query result. When **page_reverse** is set to **true**, this parameter is used together to query resources on the previous page.
next_marker	String	Specifies the ID of the last record in the pagination query result.
current_count	Integer	Specifies the number of records.

Example Requests

Querying load balancer flavors

```
GET https://{ELB_Endpoint}/v3/057ef081eb00d2732fd1c01a9be75e6f/elb/flavors?
limit=2&marker=179568ef-5ba4-4ca0-8c5e-5d581db779b1
```

Example Responses

Status code: 200

Successful request.

```
{
  "request_id" : "01e84c2750b7217e5903b3d3bc9a9fda",
```



```
"flavors" : [ {
  "name" : "L7_flavor.basic.elb.s1.small",
  "shared" : true,
  "project_id" : "060576798a80d5762fafc01a9b5eedc7",
  "info" : {
    "bandwidth" : 50000,
    "connection" : 200000,
    "cps" : 2000,
    "https_cps" : 200,
    "lcu" : 10,
    "qps" : 4000
  },
  "id" : "037418d4-8c9e-40b8-9e54-70ff4848fd82",
  "type" : "L7_basic",
  "flavor_sold_out" : false,
  "public_border_group" : "center",
  "category" : 0
}, {
  "name" : "L4_flavor.elb.s2.small",
  "shared" : true,
  "project_id" : "8d53f081ea24444aa95e2bfa942ef6ee",
  "info" : {
    "bandwidth" : 100000,
    "connection" : 1000000,
    "cps" : 20000,
    "lcu" : 20
  },
  "id" : "03925294-4ae2-4cdb-b912-cf171e782095",
  "type" : "L4",
  "flavor_sold_out" : false,
  "public_border_group" : "center",
  "category" : 0
} ],
"page_info" : {
  "next_marker" : "03925294-4ae2-4cdb-b912-cf171e782095",
  "previous_marker" : "037418d4-8c9e-40b8-9e54-70ff4848fd82",
  "current_count" : 2
}
}
```


Status Codes

Status Code	Description
200	Successful request.

Error Codes

See **Error Codes**.

5.4.2 Viewing the Details of a Flavor

Function

This API is used to view the details of a flavor.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/flavors/{flavor_id}

Table 5-24 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
flavor_id	Yes	String	Specifies the flavor ID.

Request Parameters

Table 5-25 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-26 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
flavor	**Flavor** object	Specifies the flavor.

Table 5-27 Flavor

Parameter	Type	Description
id	String	Specifies the flavor ID.
info	**FlavorInfo** object	Specifies the flavor metrics.

Parameter	Type	Description
name	String	Specifies the flavor name. Network load balancers have the following flavors: • L4_flavor.elb.s1.small: small I • L4_flavor.elb.s2.small: small II • L4_flavor.elb.s1.medium: medium I • L4_flavor.elb.s2.medium: medium II • L4_flavor.elb.s1.large: large I • L4_flavor.elb.s2.large: large II • L4_flavor.elb.pro.max: elastic flavor at Layer 4 Application load balancers have the following flavors: • L7_flavor.elb.s1.small: small I • L7_flavor.elb.s2.small: small II • L7_flavor.elb.s1.medium: medium I • L7_flavor.elb.s2.medium: medium II • L7_flavor.elb.s1.large: large I • L7_flavor.elb.s2.large: large II • L7_flavor.elb.s1.extra-large: extra-large I • L7_flavor.elb.s2.extra-large: extra-large II • L7_flavor.elb.pro.max: elastic flavor at Layer 7
shared	Boolean	Specifies whether the flavor is available to all users. • **true** indicates that the flavor is available to all users. • **false** indicates that the flavor is available only to a specific user.
project_id	String	Specifies the project ID.

Parameter	Type	Description
type	String	Specifies the flavor type. The type can be: • **L4** indicates a Layer 4 flavor. • **L7** indicates a Layer 7 flavor. • **L4_elastic** indicates the minimum elastic flavor at Layer 4. This parameter has been discarded. Please do not use it. • **L7_elastic** indicates the minimum elastic flavor at Layer 7. This parameter has been discarded. Please do not use it. • **L4_elastic_max** indicates the maximum elastic flavor at Layer 4. • **L7_elastic_max** indicates the maximum elastic flavor at Layer 7.
flavor_sold_out	Boolean	Specifies whether the flavor is available. • **true** indicates the flavor is unavailable. • **false** indicates the flavor is available.
public_border_group	String	Specifies the public border group, for example, **center**.
category	Integer	Specifies the public border group code. **0** indicates **center**. **21** indicates **homezone**.

Table 5-28 FlavorInfo

Parameter	Type	Description
connection	Integer	Specifies the number of concurrent connections per second.
cps	Integer	Specifies the number of new connections per second.
qps	Integer	Specifies the number of requests per second. This parameter is available only for load balancers at Layer 7.
bandwidth	Integer	Specifies the bandwidth, in kbit/s

Parameter	Type	Description
lcu	Integer	Specifies the number of LCUs in the flavor. **NOTE** An LCU measures the dimensions on which a dedicated load balancer routes the traffic. The higher value indicates better performance.
https_cps	Integer	Specifies the number of new HTTPS connections. This parameter is available only for load balancers at Layer 7.

Example Requests

Querying the details of a flavor

```
GET https://{ELB_Endpoint}/v3/{project_id}/elb/flavors/{flavor_id}
```

Example Responses

Status code: 200

Successful request.

```
{
  "flavor" : {
    "shared" : true,
    "project_id" : "8d53f081ea24444aa95e2bfa942ef6ee",
    "info" : {
      "bandwidth" : 10000000,
      "connection" : 8000000,
      "cps" : 80000,
      "qps" : 160000,
      "lcu" : 100
    },
    "id" : "3588b525-63ed-4b8f-8a03-6aaa9ad1c36a",
    "name" : "L7_flavor.slb.s2.large",
    "type" : "L7",
    "flavor_sold_out" : false,
    "public_border_group" : "center",
    "category" : 0
  },
  "request_id" : "3b9fb516-b7bb-4760-9128-4a23dd36ae10"
}
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ShowFlavorSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowFlavorRequest request = new ShowFlavorRequest();
        request.withFlavorId("{flavor_id}");
        try {
            ShowFlavorResponse response = client.showFlavor(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowFlavorRequest()
        request.flavor_id = "{flavor_id}"
        response = client.show_flavor(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowFlavorRequest{}
    request.FlavorId = "{flavor_id}"
    response, err := client.ShowFlavor(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	Successful request.

Error Codes

See **Error Codes**.

5.5 Reserved IP Address

5.5.1 Calculating the Number of Reserved IP Addresses

Function

This API is used to calculate the number of reserved IP addresses in the following scenarios:

- To calculate the number of IP addresses required for creating a load balancer, specify **availability_zone_id** and optional parameters **l7_flavor_id**, **ip_target_enable**, and **ip_version**. Do not specify **loadbalancer_id**.
- To calculate the number of IP addresses required for adding the first HTTP or HTTPS listener to a load balancer, specify **loadbalancer_id** and do not specify other parameters.
- To calculate the number of IP addresses required for changing the flavors of a dedicated load balancer or enabling **IP as a Backend**, specify **loadbalancer_id** and **l7_flavor_id**, or specify **loadbalancer_id** and set **ip_target_enable** to **true**. You can specify **l7_flavor_id** and set **ip_target_enable** to **true** to calculate the number of IP addresses required for multiple changes.
- To calculate the number of IP addresses required for upgrading a shared load balancer, specify **loadbalancer_id** and **scene**, and do not specify other parameters.
- To calculate the number of IP addresses required for enabling **nat64_enable**, specify **nat64_enable** and **loadbalancer_id**, and do not specify other parameters.

Note:

- The number of reserved IP addresses in the query result is greater than that of the actually used IP addresses.
- The number of reserved IP addresses do not include those already assigned or in use.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/preoccupy-ip-num

Table 5-29 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Table 5-30 Query Parameters

Parameter	Mandatory	Type	Description
l7_flavor_id	No	String	Specifies the ID of the load balancer flavor at Layer 7. If this parameter is passed, the number of reserved IP addresses required for creating a dedicated load balancer with a Layer 7 flavor or for changing the Layer 7 flavor of a dedicated load balancer will be calculated. Application scenarios: creating a dedicated load balancer with a Layer 7 flavor or changing the Layer 7 flavors of a dedicated load balancer

Parameter	Mandatory	Type	Description
ip_target_enable	No	Boolean	Specifies whether to enable **IP as a Backend**. Value options: • **true**: The number of reserved IP addresses required for creating a dedicated load balancer with **IP as a Backend** enabled or for enabling **IP as a Backend** for an existing dedicated load balancer will be calculated. • **false**: The number of reserved IP addresses required for creating a dedicated load balancer with **IP as a Backend** disabled or for disabling **IP as a Backend** for an existing dedicated load balancer will be calculated. If this parameter is not passed, **IP as a Backend** is disabled. Application scenarios: creating a dedicated load balancer or creating a dedicated load balancer with **IP as a Backend** enabled or for enabling **IP as a Backend** for an existing dedicated load balancer
ip_version	No	Integer	Specifies the IP address version of the load balancer. The value can be **4** or **6**. • **4**: The number of reserved IPv4 addresses required for creating a dedicated load balancer will be calculated. • **6**: The number of reserved IPv6 addresses required for creating a dedicated load balancer will be calculated. Application scenario: creating a dedicated load balancer.

Parameter	Mandatory	Type	Description
loadbalancer_id	No	String	Specifies the load balancer ID. The number of reserved IP addresses required for changing the flavors of a load balancer or for adding the first HTTP or HTTPS listener to a load balancer will be calculated. Application scenarios: changing the flavors of a load balancer, enabling **IP as a Backend** for an existing load balancer, enabling or disabling **nat64_enable**, or adding the first HTTP or HTTPS listener to a load balancer
availability_zone_id	No	Array of strings	Calculates the number of reserved IP addresses required for creating a dedicated load balancer in the AZs specified by **availability_zone_id**. Application scenario: creating a load balancer Constraint: This parameter will not take effect when **loadbalancer_id** is passed.
scene	No	String	Calculates the number of IP addresses required for upgrading a shared load balancer to a dedicated load balancer. Constraints: **loadbalancer_id** must also be specified. Value range: **UPGRADE** (upgrading a shared load balancer to a dedicated load balancer)

Parameter	Mandatory	Type	Description
nat64_enable	No	Boolean	Specifies whether to enable **nat64_enable**. If this parameter is specified, the system will calculate the number of reserved IP addresses required for creating a load balancer whose listeners have **nat64_enable** enabled or disabled, or for enabling or disabling **nat64_enable** for the listeners of a specific load balancer. Value options: **true**: Enable **nat64_enable**. **false**: Disable **nat64_enable**. Default value: **false**

Request Parameters

Table 5-31 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-32 Response body parameters

Parameter	Type	Description
preoccupy_ip	PreoccupyIp object	Shows reserved IP address information.
request_id	String	Specifies the request ID. Note: The value is automatically generated.

Table 5-33 PreoccupyIp

Parameter	Type	Description
total	Integer	Specifies the number of preoccupied IP addresses.

Example Requests

- Querying the number of reserved IP addresses required for changing the Layer 7 flavor of a dedicated load balancer

```
https://{ELB_Endpoint}/v3/060576782980d5762f9ec014dd2f1148/elb/preoccupy-ip-num?loadbalancer_id=aff4fc31-d635-4f59-a862-edadf32e407d&l7_flavor_id=0051bc4c-a562-4b7c-953b-a250b51d992b

{
  "preoccupy_ip" : {
    "total" : 6
  },
  "request_id" : "8844e9a0-6a2d-44b7-aad9-15a7f75e4059"
}
```

- Querying the number of reserved IP addresses required for creating a dedicated load balancer that is deployed in two AZs and has **IP as a Backend** enabled

```
GET /v3/{project_id}/elb/preoccupy-ip-num?l7_flavor_id=8278944d-f92c-4393-82b2-6fb9cc1d7e53&availability_zone_id=az1&availability_zone_id=az2&ip_target_enable=true

{
  "preoccupy_ip" : {
    "total" : 20
  },
  "request_id" : "63388ec8-fa3c-4c99-b9c8-d2c83b2a9a68"
}
```

- Querying the number of reserved IP addresses required for adding the first HTTP or HTTPS listener to a dedicated load balancer

```
GET /v3/{project_id}/elb/preoccupy-ip-num?loadbalancer_id=aff4fc31-d635-4f59-a862-edadf32e407d

{
  "preoccupy_ip" : {
    "total" : 2
  },
  "request_id" : "febfce48-318d-45ba-a9d9-855462123f3b"
}
```

Example Responses

Status code: 200

Successful request.

```
{
  "preoccupy_ip" : {
    "total" : 20
  },
  "request_id" : "63388ec8-fa3c-4c99-b9c8-d2c83b2a9a68"
}
```


SDK Sample Code

The SDK sample code is as follows.

Java

- Querying the number of reserved IP addresses required for changing the Layer 7 flavor of a dedicated load balancer

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class CountPreoccupyIpNumSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        CountPreoccupyIpNumRequest request = new CountPreoccupyIpNumRequest();
        try {
            CountPreoccupyIpNumResponse response = client.countPreoccupyIpNum(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());
        }
    }
}
```

- Querying the number of reserved IP addresses required for creating a dedicated load balancer that is deployed in two AZs and has **IP as a Backend** enabled

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class CountPreoccupyIpNumSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        CountPreoccupyIpNumRequest request = new CountPreoccupyIpNumRequest();
        try {
            CountPreoccupyIpNumResponse response = client.countPreoccupyIpNum(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());
        }
    }
}
```

- Querying the number of reserved IP addresses required for adding the first HTTP or HTTPS listener to a dedicated load balancer

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class CountPreoccupyIpNumSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        CountPreoccupyIpNumRequest request = new CountPreoccupyIpNumRequest();
        try {
            CountPreoccupyIpNumResponse response = client.countPreoccupyIpNum(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

- Querying the number of reserved IP addresses required for changing the Layer 7 flavor of a dedicated load balancer

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CountPreoccupyIpNumRequest()
        response = client.count_preoccupy_ip_num(request)
        print(response)
    except exceptions.ClientRequestException as e:
```



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

- Querying the number of reserved IP addresses required for creating a dedicated load balancer that is deployed in two AZs and has **IP as a Backend** enabled

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

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

- Querying the number of reserved IP addresses required for adding the first HTTP or HTTPS listener to a dedicated load balancer

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
```



```
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CountPreoccupyIpNumRequest()
        response = client.count_preoccupy_ip_num(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

- Querying the number of reserved IP addresses required for changing the Layer 7 flavor of a dedicated load balancer

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

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

- Querying the number of reserved IP addresses required for creating a dedicated load balancer that is deployed in two AZs and has **IP as a Backend** enabled

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
```



```
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

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

- Querying the number of reserved IP addresses required for adding the first HTTP or HTTPS listener to a dedicated load balancer

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
```



```
        Build())

    request := &model.CountPreoccupyIpNumRequest{}
    response, err := client.CountPreoccupyIpNum(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	Successful request.

Error Codes

See **Error Codes**.

5.6 Load Balancer

5.6.1 Creating a Load Balancer

Function

This API is used to create a dedicated load balancer.

When you create a load balancer, note the following:

- Specify **vip_subnet_cidr_id** if you want to bind a private IPv4 address to the load balancer.
- Specify **publicip** and either **vpc_id** or **vip_subnet_cidr_id** if you want to bind a new IPv4 EIP to the load balancer.
- Specify **publicip_ids** and either **vpc_id** or **vip_subnet_cidr_id** if you want to bind an existing IPv4 EIP to the load balancer.
- Specify **ipv6_vip_virsubnet_id** if you want to bind a private IPv6 address to the load balancer.
- Specify both **ipv6_vip_virsubnet_id** and **ipv6_bandwidth** if you want to bind a public IPv6 address to the load balancer.
- Specify **l4_flavor_id** if you want to create a network load balancer and **l7_flavor_id** to create an application load balancer. Specify both **l4_flavor_id** and **l7_flavor_id** if you want to create a load balancer that can work at both Layer 4 and Layer 7.

- If **prepaid_options** is not specified, pay-per-use load balancers will be created, which are billed by fixed specifications or elastic specifications you have selected for **l4_flavor_id** and **l7_flavor_id** when creating the load balancer.

Constraints

There are some constraints when you create a dedicated load balancer:

- **vpc_id**, **vip_subnet_cidr_id**, and **ipv6_vip_virsubnet_id** cannot be left blank at the same time.
- **ip_target_enable** specifies whether to enable **IP as a Backend**. If you enable this function for a dedicated load balancer, you can associate servers in a VPC connected through a VPC peering connection, in a VPC connected through a cloud connection, or in an on-premises data center at the other end of a Direct Connect or VPN connection, by using server IP addresses.
- **admin_state_up** must be set to **true**.
- **provider** must be set to **vlb**.
- **elb_virsubnet_ids** indicates the subnets that support IPv4/IPv6 dual stack or only IPv4 subnets. If only IPv4 subnets are supported, **ipv6_vip_virsubnet_id** must be left blank.
- If you bind an EIP to the load balancer during creation, you cannot unbind it from the load balancer by calling the API after the load balancer is created. Instead, you can unbind the EIP only on the ELB console. Locate the dedicated load balancer in the load balancer list and click **More** > **Unbind EIP** in the **Operation** column.
- **publicip_ids** and **publicip** cannot be specified at the same time. Set either **publicip_ids** to bind an existing EIP to the load balancer, or **publicip** to bind a new EIP to the load balancer, or neither of them.
- If you want to add the load balancer to a shared bandwidth, you must specify the ID of the shared bandwidth. If you want the load balancer to use a new dedicated bandwidth, **charge_mode**, **share_type**, and **size** are required.

Calling Method

For details, see **Calling APIs**.

URI

POST /v3/{project_id}/elb/loadbalancers

Table 5-34 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID of the load balancer.

Request Parameters

Table 5-35 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	Specifies the token used for IAM authentication.

Table 5-36 Request body parameters

Parameter	Mandatory	Type	Description
loadbalancer	Yes	**CreateLoadBalancerOption** object	Parameters for creating a load balancer.

Table 5-37 CreateLoadBalancerOption

Parameter	Mandatory	Type	Description
project_id	No	String	Specifies the project ID.
name	No	String	Specifies the load balancer name. Note: The value can be left blank and can contain up to Unicode 255 characters, including letters and more.
description	No	String	Provides supplementary information about the load balancer. Note: The value can be left blank and can contain up to Unicode 255 characters, including letters and more.

Parameter	Mandatory	Type	Description
vip_address	No	String	Specifies the private IPv4 address bound to the load balancer. The IP address must be from the IPv4 subnet where the load balancer resides and should not be occupied. Note: • **vip_subnet_cidr_id** is required if **vip_address** is passed. • If only **vip_subnet_cidr_id** is passed, the system will automatically assign a private IPv4 address to the load balancer. • If neither **vip_address** nor **vip_subnet_cidr_id** is specified, no private IPv4 address will be assigned, and the value of **vip_address** will be **null**. The IP address must be in [0-255].[0-255].[0-255].[0-255] format, for example, 192.168.1.1.

Parameter	Mandatory	Type	Description
vip_subnet_cidr_id	No	String	Specifies the ID of the frontend IPv4 subnet where the load balancer resides. You can query parameter **neutron_subnet_id** in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets). Note: • This parameter is mandatory if you need to create a load balancer with a private IPv4 address. • **vpc_id**, **vip_subnet_cidr_id**, and **ipv6_vip_virsubnet_id** cannot be left blank at the same time. The subnet specified by **vip_subnet_cidr_id** and that specified by **ipv6_vip_virsubnet_id** must be in the VPC specified by **vpc_id**. • The subnet specified by **vip_subnet_cidr_id** must be in the VPC specified by **vpc_id** if both **vpc_id** and **vip_subnet_cidr_id** are passed. The ID must be in UUID format and can contain up to 36 characters.

Parameter	Mandatory	Type	Description
ipv6_vip_virsubnet_id	No	String	Specifies the ID of the frontend IPv6 subnet where the load balancer resides. You can query parameter **neutron_network_id** in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets). Note: • This parameter is mandatory if you need to create a load balancer with a private IPv6 address. • **vpc_id**, **vip_subnet_cidr_id**, and **ipv6_vip_virsubnet_id** cannot be left blank at the same time. The subnet specified by **vip_subnet_cidr_id** and that specified by **ipv6_vip_virsubnet_id** must be in the VPC specified by **vpc_id**. • IPv6 must have been enabled for the IPv6 subnet where the load balancer resides. The ID must be in UUID format and can contain up to 36 characters.
provider	No	String	Specifies the provider of the load balancer. The value can only be **vlb**.

Parameter	Mandatory	Type	Description
l4_flavor_id	No	String	Specifies the flavor ID of a network load balancer. You can query parameter **id** in the response by calling the API (GET https://{ELB_Endpoint}/v3/{project_id}/elb/flavors?type=L4). Note: • If neither **l4_flavor_id** nor **l7_flavor_id** is specified, the default flavor is used. The default flavor varies depending on the sites. • If **l4_flavor_id**is specified, the load balancer is billed by fixed flavor. • If **L4_elastic_max** is specified, the load balancer is billed by how many LCUs you use. The ID must be in UUID format and can contain up to 36 characters.

Parameter	Mandatory	Type	Description
l7_flavor_id	No	String	Specifies the flavor ID of the application load balancer. Note: • You can query parameter **id** in the response by calling the API (GET https://{ELB_Endpoint}/v3/{project_id}/elb/flavors?type=L7). • If neither **l4_flavor_id** nor **l7_flavor_id** is specified, the default flavor is used. The default flavor varies by site. • If the flavor type is **L7**, the load balancer uses the fixed flavor and will be billed by the specification you select. • If the flavor type is **L7_elastic_max**, the load balancer uses the elastic flavor and will be billed by how many LCUs you use. • This parameter cannot be specified when shared load balancers are created in batches. The ID must be in UUID format and can contain up to 36 characters.
guaranteed	No	Boolean	Specifies whether the load balancer is a dedicated load balancer. Value options: • **true** (default): The load balancer is a dedicated load balancer. • **false**: The load balancer is a shared load balancer. Currently, the value can only be **true**. If the value is set to **false**, 400 Bad Request will be returned.

Parameter	Mandatory	Type	Description
vpc_id	No	String	Specifies the ID of the VPC where the load balancer resides. You can query parameter **id** in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/vpcs). Note: **vpc_id**, **vip_subnet_cidr_id**, and **ipv6_vip_virsubnet_id** cannot be left blank at the same time. The subnet specified by **vip_subnet_cidr_id** and the subnet specified by **ipv6_vip_virsubnet_id** must be in the VPC specified by **vpc_id**. The ID must be in UUID format and can contain up to 36 characters.
availability_zone_list	Yes	Array of strings	Specifies the list of AZs where the load balancer can be created. You can query the AZs by calling the API (GET https://{ELB_Endpoint}/v3/{project_id}/elb/availability-zones). Select one or more AZs in the same set. **NOTE** If disaster recovery is required, you are advised to select multiple AZs.
enterprise_project_id	No	String	Specifies the ID of the enterprise project that the load balancer belongs to. The value cannot be **""**, **"0"**, or the ID of an enterprise project that does not exist. If this parameter is not passed during resource creation, the resource belongs to the default enterprise project, and **0** will be returned.

Parameter	Mandatory	Type	Description
tags	No	Array of **Tag** objects	Lists the tags added to the load balancer. Example: **"tags": [{"key":"my_tag","value":"my_tag_value"}]**
admin_state_up	No	Boolean	Specifies whether the load balancer is enabled. Value options: • **true**: indicates the load balancer is enabled. • **false**: indicates the load balancer is disabled. Default value: **true**
billing_info	No	String	Provides resource billing information. Note: • If the value is left blank, the resource is billed in pay-per-use mode. This parameter is unsupported. Please do not use it.
ipv6_bandwidth	No	**BandwidthRef** object	Specifies the ID of the bandwidth used by an IPv6 address. Note: This parameter is available only when you create or update a load balancer with a public IPv6 address. If you use a new IPv6 address and specify a shared bandwidth, the IPv6 address will be added to the shared bandwidth.
publicip_ids	No	Array of strings	Specifies the IDs of the EIP the system will automatically assign and bind to the load balancer during load balancer creation. Note: • Only the first EIP will be bound to the load balancer although multiple EIP IDs can be set.

Parameter	Mandatory	Type	Description
publicip	No	**CreateLoadBalancerPublicIpOption** object	Specifies the new EIP that will be bound to the load balancer.

Parameter	Mandatory	Type	Description
elb_virsubnet_ids	No	Array of strings	Specifies the IDs of subnets where the load balancers work. You can query parameter **neutron_network_id** in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets?vpc_id=xxxx). A load balancer uses IP addresses in such subnets to communicate with backend servers (such as in health check, and FullNAT scenarios). Note: ● The backend subnet must in the VPC where the load balancer works. ● You need to specify a backend subnet for the load balancer and add rules to the security group associated with the backend server to allow access from the backend subnet. ● If there is more than one subnet, the first subnet in the list will be used. ● If this parameter is not specified, select subnets as follows: – If IPv6 is enabled for a load balancer, the ID of subnet specified in **ipv6_vip_virsubnet_id** will be used. – If IPv4 is enabled for a load balancer, the ID of subnet specified in **vip_subnet_cidr_id** will be used. – If only public network is available for a load balancer, the ID of any

Parameter	Mandatory	Type	Description
			subnet in the VPC where the load balancer resides will be used. Subnets with more IP addresses are preferred. ● You are advised to use a dedicated subnet with sufficient IP addresses for easier O&M. ● A load balancer uses IP addresses in the backend subnet to communicate with backend servers (such as in health check, and FullNAT scenarios). To prevent traffic from being blocked by the security groups associated with backend servers, add security group rules to allow access from the backend subnet of the load balancer to backend servers. ● In the elastic scaling scenario, the reserved IP addresses may change. It is recommended that you should add security group rules to allow access from the backend subnet of the load balancer instead of certain IP addresses.

Parameter	Mandatory	Type	Description
ip_target_enable	No	Boolean	Specifies whether to add backend servers that are not in the load balancer's VPC. If you enable this function, you can add servers in a peer VPC connected through a VPC peering connection, servers in other public clouds, or servers in an on-premises data center at the other end of a Direct Connect or VPN connection, by using their IP addresses. Value options: • **true**: Enable **IP as a Backend**. • **false**: Disable **IP as a Backend**. Note: • The value can only be updated to **true**. • If you need to connect your server to a shared VPC, ensure the VPC principal has created a VPC peering connections between the two VPCs. • This function is supported only by dedicated load balancers.
deletion_protection_enable	No	Boolean	Specifies whether to enable deletion protection for the load balancer. Value options: • **true**: Enable deletion protection. • **false** (default): Disable deletion protection. **NOTE** Disable deletion protection for all your resources before deleting your account.

Parameter	Mandatory	Type	Description
prepaid_options	No	**PrepaidCreateOption** object	Shows the yearly/monthly billing information. If this parameter is passed, a yearly/monthly load balancer will be created. This parameter is unsupported. Please do not use it.
autoscaling	No	**CreateLoadbalancerAutoscalingOption** object	Specifies information about elastic scaling. If elastic scaling is enabled, the load balancer specifications can be automatically adjusted based on incoming traffic. Note: • This parameter is only available for users on the whitelist. • If elastic scaling is enabled, **l4_flavor_id** indicates the ID of the maximum elastic flavor at Layer 4. **l7_flavor_id** indicates the ID of the maximum elastic flavor at Layer 7. • This parameter has been deprecated, but is retained for compatibility purposes. Using this parameter is not recommended. If this parameter is specified, the load balancer with minimum specifications will be created and you will be billed for the minimum specifications.

Parameter	Mandatory	Type	Description
waf_failure_action	No	String	Specifies traffic distributing policies when the WAF is faulty. Value options: • **discard**: Traffic will not be distributed. • **forward** (default): Traffic will be distributed to the default backend servers. Note: This parameter takes effect only when WAF is enabled for the load balancer.
protection_status	No	String	Specifies the protection status. This parameter is used to prevent resources from being modified by accident on the console. If this parameter is set to **consoleProtection**, you cannot modify resource settings on the console, but you can call APIs to modify resource settings, such as resource tags. Value options: • **nonProtection** (default): The load balancer is not protected. • **consoleProtection**: **Modification Protection** is enabled on the console.
protection_reason	No	String	Specifies why the modification protection is enabled. Note: This parameter is valid only when **protection_status** is set to **consoleProtection**. The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).

Parameter	Mandatory	Type	Description
charge_mode	No	String	Specifies the charge mode when creating a load balancer. Value options: • **flavor**: billed by the fixed specification you select. • **lcu**: billed by how many LCUs you have used. Constraints: You are not recommended to specify this parameter. The charge mode will be selected based on the value you have specified for **l4_flavor_id** or **l7_flavor_id**. Note: • If this parameter is not specified during the creation of a shared load balancer, **flavor** is selected by default. • If you create a dedicated load balancer, this parameter is ignored. The charge mode will be selected based on the value you have specified for **l4_flavor_id** or **l7_flavor_id**.
ipv6_vip_address	No	String	Specifies the IPv6 address bound to the load balancer. Note: • The IPv6 address must be one in the subnet defined by **ipv6_vip_virsubnet_id**. • Subnets defined by **elb_virsubnet_ids** must support IPv4/IPv6 dual stack.

Table 5-38 Tag

Parameter	Mandatory	Type	Description
key	No	String	Specifies the tag key.

Parameter	Mandatory	Type	Description
value	No	String	Specifies the tag value.

Table 5-39 BandwidthRef

Parameter	Mandatory	Type	Description
id	Yes	String	Specifies the shared bandwidth ID.

Table 5-40 CreateLoadBalancerPublicIpOption

Parameter	Mandatory	Type	Description
ip_version	No	Integer	Specifies the IP address version. The value can be **4** (IPv4) or **6** (IPv6). The default value is **4**.
network_type	Yes	String	Specifies the EIP type. The default value is **5_bgp**. For more information, see the API for assigning an EIP in the *Virtual Private Cloud API Reference*.
billing_info	No	String	Provides billing information about the EIP. • If the value is left blank, the EIP is billed in pay-per-use mode. This parameter is unsupported. Please do not use it.
description	No	String	Provides supplementary information about the EIP.
bandwidth	Yes	**CreateLoadBalancerBandwidthOption** object	Provides supplementary information about the bandwidth.

Table 5-41 CreateLoadBalancerBandwidthOption

Parameter	Mandatory	Type	Description
name	No	String	Specifies the bandwidth name. The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods. Note: • This parameter is mandatory if **share_type** is set to **PER**. • This parameter will be ignored if the bandwidth reference has a specific ID.
size	No	Integer	Specifies the bandwidth range. The default bandwidth range is 1 Mbit/s to 2,000 Mbit/s, which may vary by region and can be viewed on the management console. Note: • This parameter is mandatory if **id** is set to **null**. • The minimum increment for bandwidth adjustment varies by bandwidth range. The following are the details: – The minimum increment is 1 Mbit/s if the bandwidth range is from 0 Mbit/s to 300 Mbit/s. – The minimum increment is 50 Mbit/s if the bandwidth range is from 301 Mbit/s to 1,000 Mbit/s. – The minimum increment is 500 Mbit/s if the bandwidth is greater than 1,000 Mbit/s.

Parameter	Mandatory	Type	Description
charge_mode	No	String	Specifies how the bandwidth used by the EIP is billed. • **traffic**: The bandwidth will be billed by traffic. • **bandwidth**: The bandwidth will be billed by fixed bandwidth. This parameter is mandatory if **id** is set to **null**.
share_type	No	String	Specifies the bandwidth type. Value options: • **PER**: indicates dedicated bandwidths. • **WHOLE**: indicates shared bandwidths. Note: • This parameter is mandatory when **id** is set to **null**. It will be ignored if the value of **id** is not **null**. • The bandwidth ID must be specified if the bandwidth type is set to **WHOLE**. • The bandwidth type cannot be **WHOLE** for IPv6 EIPs.
billing_info	No	String	Specifies bandwidth billing information. Note: This parameter is unsupported. Please do not use it.
id	No	String	Specifies the ID of the shared bandwidth to which the IP address bound to the load balancer is added. Note: • The value is the bandwidth ID when **share_type** is set to **WHOLE**.

Table 5-42 PrepaidCreateOption

Parameter	Mandatory	Type	Description
period_type	Yes	String	Specifies the subscription period. • **month**: monthly subscription • **year**: yearly subscription
period_num	No	Integer	Specifies the number of subscription periods. Value ranges: • If **period_type** is set to **month**, the value ranges from **1** to **9**. • If **period_type** is set to **year**, the value ranges from **1** to **3**.
auto_renew	No	Boolean	Specifies whether to automatically renew the subscription. • **true**: Enable automatic renewal. • **False** (default): Disable automatic renewal.
auto_pay	No	Boolean	Specifies whether the payment will be automatically deducted from the customer's account after an order is placed. • **true**: The payment will be automatically deducted from the customer's account. • **false** (default): The payment will not be automatically deducted from the customer's account. If you want to use coupons, submit your request. The system automatically will switch to the billing center, where you can use the coupons.

Table 5-43 CreateLoadbalancerAutoscalingOption

Parameter	Mandatory	Type	Description
enable	Yes	Boolean	Specifies whether to enable elastic scaling for the load balancer. The value can be **true** (elastic scaling enabled) or **false** (elastic scaling disabled).
min_l7_flavor_id	No	String	Specifies the ID of the minimum elastic flavor at Layer 7. This parameter cannot be left blank if there are HTTP or HTTPS listeners.

Response Parameters

Status code: 201

Table 5-44 Response body parameters

Parameter	Type	Description
loadbalancer	**LoadBalancer** object	Specifies the load balancer.
request_id	String	Specifies the request ID. Note: The value is automatically generated.

Table 5-45 LoadBalancer

Parameter	Type	Description
id	String	Specifies the load balancer ID.
description	String	Provides supplementary information about the load balancer.
provisioning_status	String	Specifies the provisioning status of the load balancer. Value options: • **ACTIVE**: The load balancer is successfully provisioned. • **PENDING_DELETE**: The load balancer is being deleted.

Parameter	Type	Description
admin_state_up	Boolean	Specifies whether the load balancer is enabled. Value options: • **true**: indicates the load balancer is enabled. • **false**: indicates the load balancer is disabled.
provider	String	Specifies the provider of the load balancer. The value can only be **vlb**.
pools	Array of **PoolRef** objects	Lists the IDs of backend server groups associated with the load balancer.
listeners	Array of **ListenerRef** objects	Lists the IDs of listeners added to the load balancer.
operating_status	String	Specifies the operating status of the load balancer. Value options: • **ONLINE**: indicates that the load balancer is running normally. • **FROZEN**: indicates that the load balancer is frozen.
name	String	Specifies the load balancer name.
project_id	String	Specifies the project ID of the load balancer.
vip_subnet_cidr_id	String	Specifies the ID of the frontend IPv4 subnet where the load balancer resides.
vip_address	String	Specifies the private IPv4 address bound to the load balancer.
vip_port_id	String	Specifies the ID of the port bound to the private IPv4 address of the load balancer.
tags	Array of **Tag** objects	Lists the tags added to the load balancer.
created_at	String	Specifies the time when the load balancer was created, in the format of *yyyy-MM-dd''T''HH:mm:ss''Z''*.
updated_at	String	Specifies the time when the load balancer was updated, in the format of *yyyy-MM-dd''T''HH:mm:ss''Z''*.

Parameter	Type	Description
guaranteed	Boolean	Specifies whether the load balancer is a dedicated load balancer. Value options: • **true** (default): The load balancer is a dedicated load balancer. • **false**: The load balancer is a shared load balancer.
vpc_id	String	Specifies the ID of the VPC where the load balancer resides.
eips	Array of **EipInfo** objects	Specifies the EIP bound to the load balancer. Only one EIP can be bound to a load balancer. This parameter has the same meaning as **publicips**.
ipv6_vip_address	String	Specifies the IPv6 address bound to the load balancer.
ipv6_vip_virsubnet_id	String	Specifies the ID of the IPv6 subnet where the load balancer resides.
ipv6_vip_port_id	String	Specifies the ID of the port bound to the IPv6 address of the load balancer.
availability_zone_list	Array of strings	Specifies the list of AZs where the load balancer is created.
enterprise_project_id	String	Specifies the enterprise project ID. If this parameter is not passed during resource creation, **"0"** will be returned, and the resource belongs to the default enterprise project. Note: **"0"** is not a valid enterprise project ID and cannot be used in the APIs for creating, updating the load balancer, or querying the details of the load balancer.
billing_info	String	Provides resource billing information. • If the value is left blank, the resource is billed in pay-per-use mode. This parameter is unsupported. Please do not use it.

Parameter	Type	Description
l4_flavor_id	String	Specifies the ID of a flavor at Layer 4. **l4_flavor_id** defines the maximum elastic flavor at Layer 4. Note: • If **l4_flavor_id** is specified, the load balancer is billed by fixed specifications. • If **L4_elastic_max** is specified, the load balancer is billed by how many LCUs you use.
l4_scale_flavor_id	String	Specifies the ID of the reserved flavor at Layer 4. This parameter is unsupported. Please do not use it.
l7_flavor_id	String	Specifies the ID of a flavor at Layer 7. **l7_flavor_id** defines the maximum elastic flavor at Layer 7. Note: • If **l7_flavor_id** is specified, the load balancer is billed by fixed specifications. • If **L7_elastic_max** is specified, the load balancer is billed by how many LCUs you use.
l7_scale_flavor_id	String	Specifies the ID of the reserved flavor at Layer 7. This parameter is unsupported. Please do not use it.
publicips	Array of **PublicIpInfo** objects	Specifies the EIP bound to the load balancer. Only one EIP can be bound to a load balancer. This parameter has the same meaning as **eips**.
global_eips	Array of **GlobalEipInfo** objects	Specifies the global EIP bound to the load balancer. Only the first global EIP specified under **global_eips** will be bound.
elb_virsubnet_ids	Array of strings	Lists the IDs of subnets on the downstream plane.

Parameter	Type	Description
elb_virsubnet_type	String	Specifies the type of the subnet on the downstream plane. Value options: ● **ipv4**: IPv4 subnet ● **dualstack**: subnet that supports IPv4/IPv6 dual stack
ip_target_enable	Boolean	Specifies whether to add backend servers that are not in the load balancer's VPC. If you enable this function, you can add servers in a peer VPC connected through a VPC peering connection, servers in other public clouds, or servers in an on-premises data center at the other end of a Direct Connect or VPN connection, by using their IP addresses. Value options: ● **true**: Enable **IP as a Backend**. ● **false**: Disable **IP as a Backend**. Note: ● The value can only be updated to **true**. ● If you need to connect your server to a shared VPC, ensure the VPC principal has created a VPC peering connections between the two VPCs. ● This function is supported only by dedicated load balancers.

Parameter	Type	Description
frozen_scene	String	Specifies the scenario where the load balancer is frozen. Multiple values are separated using commas (,). Value options: • **POLICE**: The load balancer is frozen due to security reasons. • **ILLEGAL**: The load balancer is frozen due to violation of laws and regulations. • **VERIFY**: Your account has not completed real-name authentication. • **PARTNER**: The load balancer is frozen by the partner. • **ARREAR**: Your account is in arrears.
ipv6_bandwidth	**BandwidthRef** object	Specifies the ID of the bandwidth used by an IPv6 address. Note: This parameter is available only when you create or update a load balancer with a public IPv6 address. If you use a new IPv6 address and specify a shared bandwidth, the IPv6 address will be added to the shared bandwidth.
deletion_protection_enable	Boolean	Specifies whether to enable deletion protection. Value options: • **true**: Enable deletion protection. • **false**: Disable deletion protection. Note: • Disable deletion protection for all your resources before deleting your account. • This parameter is returned only when deletion protection is enabled at the site.

Parameter	Type	Description
autoscaling	**AutoscalingRef** object	Specifies information about elastic scaling. If elastic scaling is enabled, the load balancer specifications can be automatically adjusted based on incoming traffic. Note: • This parameter is only available for users on the whitelist. • If elastic scaling is enabled, **l4_flavor_id** indicates the ID of the maximum elastic flavor at Layer 4. **l7_flavor_id** indicates the ID of the maximum elastic flavor at Layer 7. • This parameter has been deprecated, but is retained for compatibility purposes. Using this parameter is not recommended. If this parameter is specified, the load balancer with minimum specifications will be created and you will be billed for the minimum specifications.
public_border_group	String	Specifies the AZ group to which the load balancer belongs.
charge_mode	String	Specifies the charge mode when creating a load balancer. Value options: • **flavor**: billed by the fixed specification you select. • **lcu**: billed by how many LCUs you have used. • If this parameter is left blank: – If it is a shared load balancer, it is free. – If it is a dedicated load balancer, it will be billed by the fixed specification you select.

Parameter	Type	Description
waf_failure_action	String	Specifies traffic distributing policies when the WAF is faulty. Value options: • **discard**: Traffic will not be distributed. • **forward** (default): Traffic will be distributed to the default backend servers. Note: This parameter takes effect only when WAF is enabled for the load balancer.
protection_status	String	Specifies the protection status. Value options: • **nonProtection** (default): The load balancer is not protected. • **consoleProtection**: **Modification Protection** is enabled on the console.
protection_reason	String	Specifies why the modification protection is enabled. Note: This parameter is valid only when **protection_status** is set to **consoleProtection**. The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).
log_group_id	String	Specifies the ID of the log group that is associated with the load balancer.
log_topic_id	String	Specifies the ID of the log topic that is associated with the load balancer.

Table 5-46 PoolRef

Parameter	Type	Description
id	String	Specifies the ID of the backend server group.

Table 5-47 ListenerRef

Parameter	Type	Description
id	String	Specifies the listener ID.

Table 5-48 Tag

Parameter	Type	Description
key	String	Specifies the tag key.
value	String	Specifies the tag value.

Table 5-49 EipInfo

Parameter	Type	Description
eip_id	String	Specifies the EIP ID.
eip_address	String	Specifies the EIP.
ip_version	Integer	Specifies the IP version. **4** indicates IPv4, and **6** indicates IPv6.

Table 5-50 PublicIpInfo

Parameter	Type	Description
publicip_id	String	Specifies the EIP ID.
publicip_address	String	Specifies the IP address.
ip_version	Integer	Specifies the IP version. The value can be **4** (IPv4) or **6** (IPv6).

Table 5-51 GlobalEipInfo

Parameter	Type	Description
global_eip_id	String	Specifies the ID of the global EIP.
global_eip_address	String	Specifies the global EIP.

Parameter	Type	Description
ip_version	Integer	Specifies the IP version. The value can be **4** and **6**. **4** indicates an IPv4 address, and **6** indicates an IPv6 address.

Table 5-52 BandwidthRef

Parameter	Type	Description
id	String	Specifies the shared bandwidth ID.

Table 5-53 AutoscalingRef

Parameter	Type	Description
enable	Boolean	Specifies whether to enable elastic scaling for the load balancer. Value options: • **true**: Enable elastic scaling. • **false** (default): Disable elastic scaling.
min_l7_flavor_id	String	Specifies the ID of the minimum elastic flavor at Layer 7. Note: • This parameter cannot be left blank if there are HTTP or HTTPS listeners. • This parameter has been deprecated, but is retained for compatibility purposes. Using this parameter is not recommended. If this parameter is specified, the load balancer with minimum specifications will be created and you will be billed for the minimum specifications.

Example Requests

- Example 1: Creating a load balancer with a private IPv4 address

```
POST https://{ELB_Endpoint}/v3/060576798a80d5762fafc01a9b5eedc7/elb/loadbalancers

{
  "loadbalancer" : {
```



```
    "name" : "loadbalancer",
    "description" : "simple lb",
    "vip_subnet_cidr_id" : "1992ec06-f364-4ae3-b936-6a8cc24633b7",
    "admin_state_up" : true,
    "availability_zone_list" : [ "AZ1" ]
  }
}
```

- Example 2: Creating a load balancer with an IPv4 EIP

```
POST https://{ELB_Endpoint}/v3/060576782980d5762f9ec014dd2f1148/elb/loadbalancers

{
  "loadbalancer" : {
    "vip_subnet_cidr_id" : "e6e9271d-aef4-48f0-a93a-ccc7b09032c1",
    "availability_zone_list" : [ "AZ1" ],
    "admin_state_up" : true,
    "publicip" : {
      "network_type" : "5_bgp",
      "bandwidth" : {
        "size" : 2,
        "share_type" : "PER",
        "charge_mode" : "bandwidth",
        "name" : "bandwidth_test"
      }
    },
    "name" : "elb_eip-test"
  }
}
```

Example Responses

Status code: 201

Normal response to POST requests.

```
{
  "loadbalancer" : {
    "name" : "my_loadbalancer",
    "id" : "29cc669b-3ac8-4498-9094-bdf6193425c2",
    "project_id" : "060576798a80d5762fafc01a9b5eedc7",
    "description" : "",
    "vip_port_id" : "98697944-0cc7-4d3b-a829-001c2fb82232",
    "vip_address" : "192.168.0.214",
    "admin_state_up" : true,
    "provisioning_status" : "ACTIVE",
    "operating_status" : "ONLINE",
    "listeners" : [ ],
    "pools" : [ ],
    "tags" : [ {
      "key" : "tab_key",
      "value" : "tag1"
    } ],
    "provider" : "vlb",
    "created_at" : "2023-03-22T07:59:57Z",
    "updated_at" : "2023-03-22T07:59:59Z",
    "vpc_id" : "a1f33a4c-95b9-48a7-9350-684e2ed844b3",
    "enterprise_project_id" : "134f2181-5720-47e7-bd78-1356ed3737d6",
    "availability_zone_list" : [ ],
    "ipv6_vip_address" : null,
    "ipv6_vip_virsubnet_id" : null,
    "ipv6_vip_port_id" : null,
    "publicips" : [ {
      "publicip_id" : "3388574a-4f6f-4471-869e-97d74d21eee9",
      "publicip_address" : "88.88.87.205",
      "ip_version" : 4
    } ],
    "global_eips" : [ ],
    "elb_virsubnet_ids" : [ ],
    "elb_virsubnet_type" : null,
```



```
  "ip_target_enable" : false,
  "autoscaling" : {
    "enable" : false,
    "min_l7_flavor_id" : ""
  },
  "frozen_scene" : null,
  "public_border_group" : "center",
  "eips" : [ {
    "eip_id" : "3388574a-4f6f-4471-869e-97d74d21eee9",
    "eip_address" : "88.88.87.205",
    "ip_version" : 4
  } ],
  "guaranteed" : false,
  "billing_info" : null,
  "l4_flavor_id" : null,
  "l4_scale_flavor_id" : null,
  "l7_flavor_id" : null,
  "l7_scale_flavor_id" : null,
  "waf_failure_action" : "",
  "vip_subnet_cidr_id" : "abf31f3b-706e-4e55-a6dc-f2fcc707fd3a"
 },
 "request_id" : "bf29597181cb81b30d19f1a0115a157d"
}
```


SDK Sample Code

The SDK sample code is as follows.

Java

- Example 1: Creating a load balancer with a private IPv4 address

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;

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

public class CreateLoadBalancerSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
```

```
        CreateLoadBalancerRequest request = new CreateLoadBalancerRequest();
        CreateLoadBalancerRequestBody body = new CreateLoadBalancerRequestBody();
        List<String> listLoadbalancerAvailabilityZoneList = new ArrayList<>();
        listLoadbalancerAvailabilityZoneList.add("AZ1");
        CreateLoadBalancerOption loadbalancerbody = new CreateLoadBalancerOption();
        loadbalancerbody.withName("loadbalancer")
            .withDescription("simple lb")
            .withVipSubnetCidrId("1992ec06-f364-4ae3-b936-6a8cc24633b7")
            .withAvailabilityZoneList(listLoadbalancerAvailabilityZoneList)
            .withAdminStateUp(true);
        body.withLoadbalancer(loadbalancerbody);
        request.withBody(body);
        try {
            CreateLoadBalancerResponse response = client.createLoadBalancer(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());
        }
    }
}
```

- Example 2: Creating a load balancer with an IPv4 EIP

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;

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

public class CreateLoadBalancerSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateLoadBalancerRequest request = new CreateLoadBalancerRequest();
        CreateLoadBalancerRequestBody body = new CreateLoadBalancerRequestBody();
        CreateLoadBalancerBandwidthOption bandwidthPublicip = new CreateLoadBalancerBandwidthOption();
```



```
        bandwidthPublicip.withName("bandwidth_test")
            .withSize(2)
            .withChargeMode(CreateLoadBalancerBandwidthOption.ChargeModeEnum.fromValue("bandw
idth"))
            .withShareType(CreateLoadBalancerBandwidthOption.ShareTypeEnum.fromValue("PER"));
        CreateLoadBalancerPublicIpOption publicipLoadbalancer = new
CreateLoadBalancerPublicIpOption();
        publicipLoadbalancer.withNetworkType("5_bgp")
            .withBandwidth(bandwidthPublicip);
        List<String> listLoadbalancerAvailabilityZoneList = new ArrayList<>();
        listLoadbalancerAvailabilityZoneList.add("AZ1");
        CreateLoadBalancerOption loadbalancerbody = new CreateLoadBalancerOption();
        loadbalancerbody.withName("elb_eip-test")
            .withVipSubnetCidrId("e6e9271d-aef4-48f0-a93a-ccc7b09032c1")
            .withAvailabilityZoneList(listLoadbalancerAvailabilityZoneList)
            .withAdminStateUp(true)
            .withPublicip(publicipLoadbalancer);
        body.withLoadbalancer(loadbalancerbody);
        request.withBody(body);
        try {
            CreateLoadBalancerResponse response = client.createLoadBalancer(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

- Example 1: Creating a load balancer with a private IPv4 address

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateLoadBalancerRequest()
        listAvailabilityZoneListLoadbalancer = [
            "AZ1"
```



```
        ]
        loadbalancerbody = CreateLoadBalancerOption(
            name="loadbalancer",
            description="simple lb",
            vip_subnet_cidr_id="1992ec06-f364-4ae3-b936-6a8cc24633b7",
            availability_zone_list=listAvailabilityZoneListLoadbalancer,
            admin_state_up=True
        )
        request.body = CreateLoadBalancerRequestBody(
            loadbalancer=loadbalancerbody
        )
        response = client.create_load_balancer(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

- Example 2: Creating a load balancer with an IPv4 EIP

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateLoadBalancerRequest()
        bandwidthPublicip = CreateLoadBalancerBandwidthOption(
            name="bandwidth_test",
            size=2,
            charge_mode="bandwidth",
            share_type="PER"
        )
        publicipLoadbalancer = CreateLoadBalancerPublicIpOption(
            network_type="5_bgp",
            bandwidth=bandwidthPublicip
        )
        listAvailabilityZoneListLoadbalancer = [
            "AZ1"
        ]
        loadbalancerbody = CreateLoadBalancerOption(
            name="elb_eip-test",
            vip_subnet_cidr_id="e6e9271d-aef4-48f0-a93a-ccc7b09032c1",
            availability_zone_list=listAvailabilityZoneListLoadbalancer,
            admin_state_up=True,
            publicip=publicipLoadbalancer
        )
        request.body = CreateLoadBalancerRequestBody(
            loadbalancer=loadbalancerbody
```



```
        )
        response = client.create_load_balancer(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

- Example 1: Creating a load balancer with a private IPv4 address

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateLoadBalancerRequest{}
    var listAvailabilityZoneListLoadbalancer = []string{
        "AZ1",
    }
    nameLoadbalancer:= "loadbalancer"
    descriptionLoadbalancer:= "simple lb"
    vipSubnetCidrIdLoadbalancer:= "1992ec06-f364-4ae3-b936-6a8cc24633b7"
    adminStateUpLoadbalancer:= true
    loadbalancerbody := &model.CreateLoadBalancerOption{
        Name: &nameLoadbalancer,
        Description: &descriptionLoadbalancer,
        VipSubnetCidrId: &vipSubnetCidrIdLoadbalancer,
        AvailabilityZoneList: listAvailabilityZoneListLoadbalancer,
        AdminStateUp: &adminStateUpLoadbalancer,
    }
    request.Body = &model.CreateLoadBalancerRequestBody{
        Loadbalancer: loadbalancerbody,
    }
    response, err := client.CreateLoadBalancer(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
```



```
    }
}
```

- Example 2: Creating a load balancer with an IPv4 EIP

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateLoadBalancerRequest{}
    nameBandwidth:= "bandwidth_test"
    sizeBandwidth:= int32(2)
    chargeModeBandwidth:= model.GetCreateLoadBalancerBandwidthOptionChargeModeEnum().BANDWIDTH
    shareTypeBandwidth:= model.GetCreateLoadBalancerBandwidthOptionShareTypeEnum().PER
    bandwidthPublicip := &model.CreateLoadBalancerBandwidthOption{
        Name: &nameBandwidth,
        Size: &sizeBandwidth,
        ChargeMode: &chargeModeBandwidth,
        ShareType: &shareTypeBandwidth,
    }
    publicipLoadbalancer := &model.CreateLoadBalancerPublicIpOption{
        NetworkType: "5_bgp",
        Bandwidth: bandwidthPublicip,
    }
    var listAvailabilityZoneListLoadbalancer = []string{
        "AZ1",
    }
    nameLoadbalancer:= "elb_eip-test"
    vipSubnetCidrIdLoadbalancer:= "e6e9271d-aef4-48f0-a93a-ccc7b09032c1"
    adminStateUpLoadbalancer:= true
    loadbalancerbody := &model.CreateLoadBalancerOption{
        Name: &nameLoadbalancer,
        VipSubnetCidrId: &vipSubnetCidrIdLoadbalancer,
        AvailabilityZoneList: listAvailabilityZoneListLoadbalancer,
        AdminStateUp: &adminStateUpLoadbalancer,
        Publicip: publicipLoadbalancer,
    }
    request.Body = &model.CreateLoadBalancerRequestBody{
        Loadbalancer: loadbalancerbody,
    }
    response, err := client.CreateLoadBalancer(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 POST requests.

Error Codes

See **Error Codes**.

5.6.2 Batch Creating Load Balancers

Function

This API is used to create dedicated or shared load balancers in batches.

When you create load balancers, note the following:

- Specify **vip_subnet_cidr_id** if you want to bind private IPv4 addresses to the load balancers.
- Specify **publicip** and either **vpc_id** or **vip_subnet_cidr_id** if you want to bind new IPv4 EIPs to the load balancers.
- Specify **publicip_ids** and either **vpc_id** or **vip_subnet_cidr_id** if you want to bind existing IPv4 EIPs to the load balancers.
- Specify **ipv6_vip_virsubnet_id** if you want to bind private IPv6 addresses to the load balancers.
- Specify both **ipv6_vip_virsubnet_id** and **ipv6_bandwidth** if you want to bind public IPv6 addresses to the load balancers.
- Specify **l4_flavor_id** if you want to create network load balancers and **l7_flavor_id** to create application load balancers. Specify both **l4_flavor_id** and **l7_flavor_id** if you want to create load balancers that can work at both Layer 4 and Layer 7.
- Do not specify **publicip_ids**, **vip_address**, or **ipv6_vip_address** when creating load balancers in batches. You cannot bind existing private IPv4 addresses, IPv6 addresses, or public IP addresses to the load balancers.
- If **prepaid_options** is not specified, pay-per-use load balancers will be created, which are billed by fixed specifications or elastic specifications you have selected for **l4_flavor_id** and **l7_flavor_id** when creating the load balancers.

- This is an asynchronous API, returning load balancer IDs and job IDs in its response body. You can use the job ID to query the load balancer creation progress.
- The rules for specifying parameters in the request body are different when you create dedicated and shared load balancers in batches. For details, see the description of each parameter in the request body.

Constraints

There are some constraints when you create load balancers:

- **vpc_id**, **vip_subnet_cidr_id**, and **ipv6_vip_virsubnet_id** cannot be left blank at the same time.
- If the value of **number** is greater than 1, do not specify **publicip_ids**, **vip_address**, and **ipv6_vip_address**.
- **ip_target_enable** specifies whether to enable **IP as a Backend**. If you set it to **true**, you can associate servers in a VPC connected through a VPC peering connection, in a VPC connected through a cloud connection, or in an on-premises data center at the other end of a Direct Connect or VPN connection, by using server IP addresses. If you set it to **false**, the load balancer and the backend servers must be in the same VPC.
- **admin_state_up** must be **true**.
- **provider** must be set to **vlb**.
- **elb_virsubnet_ids** indicates the subnets that support IPv4/IPv6 dual stack or only IPv4. If only IPv4 subnets are supported, **ipv6_vip_virsubnet_id** must be left blank.
- If you bind an EIP to the load balancer during creation, you cannot unbind it from the load balancer by calling the API after the load balancer is created. Instead, you can unbind the EIP only on the ELB console. Locate the load balancer in the load balancer list and click **More** > **Unbind EIP** in the **Operation** column.
- **publicip_ids** and **publicip** cannot be specified at the same time. Set either **publicip_ids** to bind an existing EIP to the load balancer, or **publicip** to bind a new EIP to the load balancer, or neither of them.
- If you want to add the load balancer to a shared bandwidth, you must specify the ID of the shared bandwidth. If you want the load balancer to use a new dedicated bandwidth, **charge_mode**, **share_type**, and **size** are required.
- You cannot bind an existing and unoccupied private IPv4 address, IPv6 address, or public IPv6 address to load balancers.

Calling Method

For details, see **Calling APIs**.

URI

POST /v3/{project_id}/elb/loadbalancers/batch-create

Table 5-54 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the ID of the project where the load balancer is used.

Request Parameters

Table 5-55 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	Specifies the token used for IAM authentication.

Table 5-56 Request body parameters

Parameter	Mandatory	Type	Description
loadbalancer	Yes	**BatchCreateLoadBalancerOption** object	Specifies the load balancer.

Table 5-57 BatchCreateLoadBalancerOption

Parameter	Mandatory	Type	Description
id	No	String	Specifies the ID of the load balancer. This parameter is unsupported. Please do not use it.
ids	No	Array of strings	Specifies the IDs of the load balancers created in batches. This parameter is unsupported. Please do not use it.
project_id	No	String	Specifies the ID of the project where the load balancer is used.
number	No	Integer	Specifies the number of load balancers to be created.

Parameter	Mandatory	Type	Description
name	No	String	Specifies the load balancer names. Note: • If the number of load balancers to be created is 1, the load balancer name is the value defined by **name**. • If the number of load balancers to be created is greater than 1, each name is suffixed with a 4-digit number. For example, if you create three load balancers and set **name** to **elb-test**, the names of these load balancers are **elb-test-0001**, **elb-test-0002**, and **elb-test-0003**.
description	No	String	Specifies the descriptions of these load balancers.

Parameter	Mandatory	Type	Description
vip_address	No	String	Specifies the virtual IPv4 address bound to the load balancer. The IP address must be from the IPv4 subnet where the load balancer resides and should not be used by other services. Note: • **vip_subnet_cidr_id** is also required if **vip_address** is specified. • If only **vip_subnet_cidr_id** is specified, the system will automatically assign a private IPv4 address to the load balancer. • If neither **vip_address** nor **vip_subnet_cidr_id** is specified, no private IPv4 address will be assigned, and the value of **vip_address** will be **null**. • If the value of **number** is greater than 1, this parameter cannot be specified and error code 400 will be returned.

Parameter	Mandatory	Type	Description
vip_subnet_cidr_id	No	String	Specifies the ID of the IPv4 subnet where the load balancer works. This parameter is mandatory if you need to create a load balancer with a virtual IPv4 address. You can query parameter **neutron_subnet_id** in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets) Note: • **vpc_id**, **vip_subnet_cidr_id**, and **ipv6_vip_virsubnet_id** cannot be left blank at the same time. The subnet specified by **vip_subnet_cidr_id** and the subnet specified by **ipv6_vip_virsubnet_id** must be in the VPC specified by **vpc_id**. • The subnet specified by **vip_subnet_cidr_id** must be in the VPC specified by **vpc_id** if both **vpc_id** and **vip_subnet_cidr_id** are specified.

Parameter	Mandatory	Type	Description
ipv6_vip_virsubnet_id	No	String	Specifies the ID of the IPv6 subnet where the load balancer works. You can query parameter **neutron_network_id** in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets). Note: • **vpc_id**, **vip_subnet_cidr_id**, and **ipv6_vip_virsubnet_id** cannot be left blank at the same time. The subnet specified by **vip_subnet_cidr_id** and the subnet specified by **ipv6_vip_virsubnet_id** must be in the VPC specified by **vpc_id**. • IPv6 must have been enabled for the subnet where the load balancer resides. • This parameter cannot be specified when shared load balancers are created in batches.
provider	No	String	Specifies the provider of the load balancer. The value is fixed to **vlb**. This parameter cannot be specified when shared load balancers are created in batches.

Parameter	Mandatory	Type	Description
l4_flavor_id	No	String	Specifies the flavor ID of the network load balancer. Note: • You can query parameter **id** in the response by calling the API (GET https://{ELB_Endpoint}/v3/{project_id}/elb/flavors?type=L4). • If neither **l4_flavor_id** nor **l7_flavor_id** is specified, the default flavor is used. The default flavor varies by site. • If the flavor type is **L4**, the load balancer uses the fixed flavor and will be billed by the specification you select. • If the flavor type is **L4_elastic_max**, the load balancer uses the elastic flavor and will be billed by how many LCUs you use. • This parameter cannot be specified when shared load balancers are created in batches.

Parameter	Mandatory	Type	Description
l7_flavor_id	No	String	Specifies the flavor ID of the application load balancer. Note: • You can query parameter **id** in the response by calling the API (GET https://{ELB_Endpoint}/v3/{project_id}/elb/flavors?type=L7). • If neither **l4_flavor_id** nor **l7_flavor_id** is specified, the default flavor is used. The default flavor varies by site. • If the flavor type is **L7**, the load balancer uses the fixed flavor and will be billed by the specification you select. • If the flavor type is **L7_elastic_max**, the load balancer uses the elastic flavor and will be billed by how many LCUs you use. • This parameter cannot be specified when shared load balancers are created in batches.
guaranteed	No	Boolean	Specifies whether to create dedicated or shared load balancers. Value options: • **true**: Create dedicated load balancers. • **false**: Create shared load balancers. Default value: **true**

Parameter	Mandatory	Type	Description
vpc_id	No	String	Specifies the ID of the VPC where the load balancer resides. You can query parameter **id** in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/vpcs). Note: • **vpc_id**, **vip_subnet_cidr_id**, and **ipv6_vip_virsubnet_id** cannot be left blank at the same time. The subnet specified by **vip_subnet_cidr_id** and the subnet specified by **ipv6_vip_virsubnet_id** must be in the VPC specified by **vpc_id**. • This parameter cannot be specified when shared load balancers are created in batches.
availability_zone_list	Yes	Array of strings	Specifies the list of AZs where the load balancer can be created. You can query the AZs by calling the API (GET https://{ELB_Endpoint}/v3/{project_id}/elb/availability-zones). Select one or more AZs in the same set. Note: This parameter cannot be specified when shared load balancers are created in batches.
enterprise_project_id	No	String	Specifies the ID of the enterprise project where the load balancer is used. The value cannot be **""**, **"0"**, or the ID of an enterprise project that does not exist. If this parameter is not passed during resource creation, the resource belongs to the default enterprise project, and **0** will be returned.

Parameter	Mandatory	Type	Description
tags	No	Array of **Tag** objects	Specifies the tags added to the load balancer. Example: **"tags": [{"key":"my_tag","value":"my_tag_value"}]**
admin_state_up	No	Boolean	Specifies whether the load balancer is enabled. Value options: • **true**: indicates the load balancer is enabled. • **false**: indicates the load balancer is disabled. Default value: **true**
ipv6_bandwidth	No	**BandwidthRef** object	This parameter cannot be specified when shared load balancers are created in batches.
bandwidth	No	**BandwidthRef** object	This parameter cannot be specified when dedicated load balancers are created in batches.
publicip_ids	No	Array of strings	Specifies the ID of the EIP bound to the load balancer. Only the first EIP in the array will be bound. If the value of **number** is greater than 1, this parameter cannot be specified and error code 400 will be returned.
publicip	No	**CreateLoadBalancerPublicIpOption** object	Specifies the new EIP that will be bound to the load balancer.

Parameter	Mandatory	Type	Description
elb_virsubnet_ids	No	Array of strings	Specifies the IDs of subnets on the downstream plane. You can query parameter **neutron_network_id** in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets). If this parameter is not specified, the subnet IDs will be used based on the following rules: • If IPv6 is enabled for a load balancer, the subnet IDs specified in **ipv6_vip_virsubnet_id** will be used. • If IPv6 is not enabled for a load balancer, the subnet IDs specified in **vip_subnet_cidr_id** will be used. • If a load balancer only works on the public network, the ID of any subnet in the VPC where the load balancer is deployed will be used. The subnets that have the most available IP addresses are preferred. • This parameter cannot be specified when shared load balancers are created in batches. If there is more than one subnet, the first subnet in the list will be used to assign IP addresses. The subnets must be in the VPC where the load balancer works.

Parameter	Mandatory	Type	Description
ip_target_enable	No	Boolean	Specifies whether to add backend servers that are not in the load balancer's VPC. If you enable this function, you can add servers in a peer VPC connected through a VPC peering connection, servers in other public clouds, or servers in an on-premises data center at the other end of a Direct Connect or VPN connection, by using their IP addresses. Value options: • **true**: Enable **ip_target_enable**. • **false**: Disable **ip_target_enable**. Note: • The value can only be updated to **true**. • If you need to connect your server to a shared VPC, ensure the VPC principal has created a VPC peering connections between the two VPCs. • This function is supported only by dedicated load balancers.
deletion_protection_enable	No	Boolean	Specifies whether to enable deletion protection. This parameter cannot be specified when shared load balancers are created in batches. Value options: • **true**: Enable deletion protection. • **false** (default): Disable deletion protection. **NOTE** Disable deletion protection for all your resources before deleting your account.

Parameter	Mandatory	Type	Description
autoscaling	No	**CreateLoadbalancerAutoscalingOption** object	Specifies information about elastic scaling. If elastic scaling is enabled, the load balancer specifications can be automatically adjusted based on incoming traffic. Note: • This parameter is only available for users on the whitelist. • If elastic scaling is enabled, **l4_flavor_id** indicates the ID of the maximum elastic flavor at Layer 4. **l7_flavor_id** indicates the ID of the maximum elastic flavor at Layer 7. • This parameter has been deprecated, but is retained for compatibility purposes. Using this parameter is not recommended. If this parameter is specified, the load balancer with minimum specifications will be created and you will be billed for the minimum specifications.
waf_failure_action	No	String	Specifies traffic distributing policies when the WAF is faulty. • **discard**: Traffic will not be distributed. • **forward**: Traffic will be distributed to the default backend servers. Note: This parameter takes effect only when WAF is enabled for the load balancer.

Parameter	Mandatory	Type	Description
protection_status	No	String	Specifies the protection status. Value options: • **nonProtection** (default): The load balancer is not protected. • **consoleProtection**: **Modification Protection** is enabled on the console.
protection_reason	No	String	Specifies why the modification protection is enabled. Note: This parameter is valid only when **protection_status** is set to **consoleProtection**. The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).
ipv6_vip_address	No	String	Specifies the IPv6 address bound to the load balancer. If the value of **number** is greater than 1, this parameter cannot be specified and error code 400 will be returned. This parameter cannot be specified when shared load balancers are created in batches.

Table 5-58 Tag

Parameter	Mandatory	Type	Description
key	No	String	Specifies the tag key.
value	No	String	Specifies the tag value.

Table 5-59 BandwidthRef

Parameter	Mandatory	Type	Description
id	Yes	String	Specifies the shared bandwidth ID.

Table 5-60 CreateLoadBalancerPublicIpOption

Parameter	Mandatory	Type	Description
ip_version	No	Integer	Specifies the IP address version. The value can be **4** (IPv4) or **6** (IPv6). The default value is **4**.
network_type	Yes	String	Specifies the EIP type. The default value is **5_bgp**. For more information, see the API for assigning an EIP in the *Virtual Private Cloud API Reference*.
billing_info	No	String	Provides billing information about the EIP. • If the value is left blank, the EIP is billed in pay-per-use mode. This parameter is unsupported. Please do not use it.
description	No	String	Provides supplementary information about the EIP.
bandwidth	Yes	**CreateLoadBalancerBandwidthOption** object	Provides supplementary information about the bandwidth.

Table 5-61 CreateLoadBalancerBandwidthOption

Parameter	Mandatory	Type	Description
name	No	String	Specifies the bandwidth name. The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods. Note: • This parameter is mandatory if **share_type** is set to **PER**. • This parameter will be ignored if the bandwidth reference has a specific ID.

Parameter	Mandatory	Type	Description
size	No	Integer	Specifies the bandwidth range. The default bandwidth range is 1 Mbit/s to 2,000 Mbit/s, which may vary by region and can be viewed on the management console. Note: • This parameter is mandatory if **id** is set to **null**. • The minimum increment for bandwidth adjustment varies by bandwidth range. The following are the details: – The minimum increment is 1 Mbit/s if the bandwidth range is from 0 Mbit/s to 300 Mbit/s. – The minimum increment is 50 Mbit/s if the bandwidth range is from 301 Mbit/s to 1,000 Mbit/s. – The minimum increment is 500 Mbit/s if the bandwidth is greater than 1,000 Mbit/s.
charge_mode	No	String	Specifies how the bandwidth used by the EIP is billed. • **traffic**: The bandwidth will be billed by traffic. • **bandwidth**: The bandwidth will be billed by fixed bandwidth. This parameter is mandatory if **id** is set to **null**.

Parameter	Mandatory	Type	Description
share_type	No	String	Specifies the bandwidth type. Value options: • **PER**: indicates dedicated bandwidths. • **WHOLE**: indicates shared bandwidths. Note: • This parameter is mandatory when **id** is set to **null**. It will be ignored if the value of **id** is not **null**. • The bandwidth ID must be specified if the bandwidth type is set to **WHOLE**. • The bandwidth type cannot be **WHOLE** for IPv6 EIPs.
billing_info	No	String	Specifies bandwidth billing information. Note: This parameter is unsupported. Please do not use it.
id	No	String	Specifies the ID of the shared bandwidth to which the IP address bound to the load balancer is added. Note: • The value is the bandwidth ID when **share_type** is set to **WHOLE**.

Table 5-62 CreateLoadbalancerAutoscalingOption

Parameter	Mandatory	Type	Description
enable	Yes	Boolean	Specifies whether to enable elastic scaling for the load balancer. The value can be **true** (elastic scaling enabled) or **false** (elastic scaling disabled).

Parameter	Mandatory	Type	Description
min_l7_flavor_id	No	String	Specifies the ID of the minimum elastic flavor at Layer 7. This parameter cannot be left blank if there are HTTP or HTTPS listeners.

Response Parameters

Status code: 202

Table 5-63 Response body parameters

Parameter	Type	Description
loadbalancer_ids	Array of strings	Specifies the IDs of the load balancers created in batches.
job_id	String	Specifies task ID of the batch creation.
request_id	String	Specifies the request ID. Note: The value is automatically generated.

Example Requests

- Example 1: Creating three pay-per-use, dedicated load balancers and binding private IPv4 addresses to them

```
POST https://{ELB_Endpoint}/v3/060576798a80d5762fafc01a9b5eedc7/elb/loadbalancers/batch-create

{
  "loadbalancer" : {
    "name" : "loadbalancer",
    "description" : "simple batch create lb",
    "vip_subnet_cidr_id" : "1992ec06-f364-4ae3-b936-6a8cc24633b7",
    "admin_state_up" : true,
    "availability_zone_list" : [ "AZ1" ],
    "number" : 3
  }
}
```

- Example 1: Creating three shared load balancers and binding private IPv4 addresses to them

```
POST https://{ELB_Endpoint}/v3/060576798a80d5762fafc01a9b5eedc7/elb/loadbalancers/batch-create

{
  "loadbalancer" : {
    "name" : "loadbalancer",
    "description" : "simple batch create lb",
    "availability_zone_list" : [ "AZ1" ],
    "vip_subnet_cidr_id" : "1992ec06-f364-4ae3-b936-6a8cc24633b7",
    "admin_state_up" : true,
    "guaranteed" : false,
    "number" : 3
```



```
  }
}
```

Example Responses

Status code: 202

Normal response

```
{
  "job_id" : "060576798a80d5762fafc01a9b5eedc7",
  "loadbalancer_ids" : [ "de7946ba-3b77-4119-8338-acc25eb05611", "ba27f70b-b52f-4a77-9220-fd15726e50bd" ],
  "request_id" : "bf29597181cb81b30d19f1a0115a157d"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

- Example 1: Creating three pay-per-use, dedicated load balancers and binding private IPv4 addresses to them

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;

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

public class BatchCreateLoadBalancersSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        BatchCreateLoadBalancersRequest request = new BatchCreateLoadBalancersRequest();
        BatchCreateLoadBalancersRequestBody body = new BatchCreateLoadBalancersRequestBody();
        List<String> listLoadbalancerAvailabilityZoneList = new ArrayList<>();
        listLoadbalancerAvailabilityZoneList.add("AZ1");
        BatchCreateLoadBalancerOption loadbalancerbody = new BatchCreateLoadBalancerOption();
        loadbalancerbody.withNumber(3)
```



```
            .withName("loadbalancer")
            .withDescription("simple batch create lb")
            .withVipSubnetCidrId("1992ec06-f364-4ae3-b936-6a8cc24633b7")
            .withAvailabilityZoneList(listLoadbalancerAvailabilityZoneList)
            .withAdminStateUp(true);
        body.withLoadbalancer(loadbalancerbody);
        request.withBody(body);
        try {
            BatchCreateLoadBalancersResponse response = client.batchCreateLoadBalancers(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());
        }
    }
}
```

- Example 1: Creating three shared load balancers and binding private IPv4 addresses to them

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;

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

public class BatchCreateLoadBalancersSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        BatchCreateLoadBalancersRequest request = new BatchCreateLoadBalancersRequest();
        BatchCreateLoadBalancersRequestBody body = new BatchCreateLoadBalancersRequestBody();
        List<String> listLoadbalancerAvailabilityZoneList = new ArrayList<>();
        listLoadbalancerAvailabilityZoneList.add("AZ1");
        BatchCreateLoadBalancerOption loadbalancerbody = new BatchCreateLoadBalancerOption();
        loadbalancerbody.withNumber(3)
            .withName("loadbalancer")
```



```
            .withDescription("simple batch create lb")
            .withVipSubnetCidrId("1992ec06-f364-4ae3-b936-6a8cc24633b7")
            .withGuaranteed(false)
            .withAvailabilityZoneList(listLoadbalancerAvailabilityZoneList)
            .withAdminStateUp(true);
        body.withLoadbalancer(loadbalancerbody);
        request.withBody(body);
        try {
            BatchCreateLoadBalancersResponse response = client.batchCreateLoadBalancers(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

- Example 1: Creating three pay-per-use, dedicated load balancers and binding private IPv4 addresses to them

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = BatchCreateLoadBalancersRequest()
        listAvailabilityZoneListLoadbalancer = [
            "AZ1"
        ]
        loadbalancerbody = BatchCreateLoadBalancerOption(
            number=3,
            name="loadbalancer",
            description="simple batch create lb",
            vip_subnet_cidr_id="1992ec06-f364-4ae3-b936-6a8cc24633b7",
            availability_zone_list=listAvailabilityZoneListLoadbalancer,
            admin_state_up=True
        )
        request.body = BatchCreateLoadBalancersRequestBody(
```



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

- Example 1: Creating three shared load balancers and binding private IPv4 addresses to them

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = BatchCreateLoadBalancersRequest()
        listAvailabilityZoneListLoadbalancer = [
            "AZ1"
        ]
        loadbalancerbody = BatchCreateLoadBalancerOption(
            number=3,
            name="loadbalancer",
            description="simple batch create lb",
            vip_subnet_cidr_id="1992ec06-f364-4ae3-b936-6a8cc24633b7",
            guaranteed=False,
            availability_zone_list=listAvailabilityZoneListLoadbalancer,
            admin_state_up=True
        )
        request.body = BatchCreateLoadBalancersRequestBody(
            loadbalancer=loadbalancerbody
        )
        response = client.batch_create_load_balancers(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

- Example 1: Creating three pay-per-use, dedicated load balancers and binding private IPv4 addresses to them

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.BatchCreateLoadBalancersRequest{}
    var listAvailabilityZoneListLoadbalancer = []string{
        "AZ1",
    }
    numberLoadbalancer:= int32(3)
    nameLoadbalancer:= "loadbalancer"
    descriptionLoadbalancer:= "simple batch create lb"
    vipSubnetCidrIdLoadbalancer:= "1992ec06-f364-4ae3-b936-6a8cc24633b7"
    adminStateUpLoadbalancer:= true
    loadbalancerbody := &model.BatchCreateLoadBalancerOption{
        Number: &numberLoadbalancer,
        Name: &nameLoadbalancer,
        Description: &descriptionLoadbalancer,
        VipSubnetCidrId: &vipSubnetCidrIdLoadbalancer,
        AvailabilityZoneList: listAvailabilityZoneListLoadbalancer,
        AdminStateUp: &adminStateUpLoadbalancer,
    }
    request.Body = &model.BatchCreateLoadBalancersRequestBody{
        Loadbalancer: loadbalancerbody,
    }
    response, err := client.BatchCreateLoadBalancers(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

- Example 1: Creating three shared load balancers and binding private IPv4 addresses to them

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
```



```
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.BatchCreateLoadBalancersRequest{}
    var listAvailabilityZoneListLoadbalancer = []string{
        "AZ1",
    }
    numberLoadbalancer:= int32(3)
    nameLoadbalancer:= "loadbalancer"
    descriptionLoadbalancer:= "simple batch create lb"
    vipSubnetCidrIdLoadbalancer:= "1992ec06-f364-4ae3-b936-6a8cc24633b7"
    guaranteedLoadbalancer:= false
    adminStateUpLoadbalancer:= true
    loadbalancerbody := &model.BatchCreateLoadBalancerOption{
        Number: &numberLoadbalancer,
        Name: &nameLoadbalancer,
        Description: &descriptionLoadbalancer,
        VipSubnetCidrId: &vipSubnetCidrIdLoadbalancer,
        Guaranteed: &guaranteedLoadbalancer,
        AvailabilityZoneList: listAvailabilityZoneListLoadbalancer,
        AdminStateUp: &adminStateUpLoadbalancer,
    }
    request.Body = &model.BatchCreateLoadBalancersRequestBody{
        Loadbalancer: loadbalancerbody,
    }
    response, err := client.BatchCreateLoadBalancers(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
202	Normal response

Error Codes

See **Error Codes**.

5.6.3 Upgrading a Load Balancer

Function

This API is used to upgrade a shared load balancer to a dedicated load balancer. Shared load balancers can be upgraded to dedicated load balancers, but dedicated load balancers cannot be downgraded to shared load balancers.

Calling Method

For details, see **Calling APIs**.

URI

POST /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}/upgrade

Table 5-64 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the ID of the project where the load balancer is used.
loadbalancer_id	Yes	String	Specifies the load balancer ID.

Request Parameters

Table 5-65 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Table 5-66 Request body parameters

Parameter	Mandatory	Type	Description
action	Yes	String	Specifies the action of an upgrade. • **start**: starts the upgrade. This action is supported only when **provisioning_status** of the load balancer is **ACTIVE**. • **complete**: confirms the upgrade. This action is supported only when **provision_status** of the load balancer is **UPGRADED**. After the confirmation, the operation cannot be rolled back. • **rollback**: rollbacks the upgrade. This action is supported only when **provision_status** of the load balancer is **UPGRADED**, **UPGRADE_FAILED**, or **ROLLBACK_FAILED**.
l4_flavor_id	No	String	Specifies the Layer 4 specification ID. This parameter is valid only when **action** is **start**. This parameter is mandatory when the load balancer has a Layer 4 listener. **l4_flavor_id** and **l7_flavor_id** cannot be left blank at the same time.
l7_flavor_id	No	String	Specifies the Layer 7 specification ID. This parameter is valid only when **action** is **start**. This parameter is mandatory when the load balancer has a Layer 7 listener. **l4_flavor_id** and **l7_flavor_id** cannot be left blank at the same time.

Parameter	Mandatory	Type	Description
availability_zone_list	No	Array of strings	Specifies AZs. This parameter is valid and required when **action** is **start**. You can query the AZs by calling the API (GET https://{ELB_Endpoint}/v3/{project_id}/elb/availability-zones) Select one or more AZs in the same set.
ipv6_vip_virsubnet_id	No	String	Specifies the ID of the IPv6 subnet where the load balancer works. If you want to use the load balancer to distribute IPv6 requests, this parameter is required. You can query parameter **id** in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets) Note: • The subnet defined by **ipv6_vip_virsubnet_id** must in the VPC to which the original shared load balancer works. • IPv6 must be enabled for the subnet defined by **ipv6_vip_virsubnet_id**.

Parameter	Mandatory	Type	Description
ipv6_vip_address	No	String	Specifies the virtual IPv6 address bound to the load balancer. The IP address must be from the IPv6 subnet where the load balancer resides and should not be used by other services. Note: • **ipv6_vip_virsubnet_id** is also required if **ipv6_vip_address** is specified. • If only **ipv6_vip_virsubnet_id** is specified, the system will automatically assign a private IPv6 address to the load balancer. • If neither **ipv6_vip_address** nor **ipv6_vip_virsubnet_id** is specified, no private IPv6 address will be assigned, and the value of **ipv6_vip_address** will be **null**.
elb_virsubnet_ids	No	Array of strings	Specifies the IDs of subnets on the downstream plane. This parameter is valid only when **action** is **start**. You can query parameter **neutron_network_id** in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets). If this parameter is not specified, the subnet IDs specified in **vip_subnet_cidr_id** will be used. The subnets must be in the VPC where the load balancer works.

Parameter	Mandatory	Type	Description
prepaid_options	No	UpgradePrepaidOption object	Shows the yearly/monthly billing information. If this parameter is passed, a yearly/monthly load balancer will be created. This parameter is unsupported. Please do not use it.

Table 5-67 UpgradePrepaidOption

Parameter	Mandatory	Type	Description
period_type	Yes	String	Specifies the subscription period type. Value options: • **month**: monthly subscription • **year**: yearly subscription
period_num	No	Integer	Specifies the number of subscription periods. Value options: • The value ranges from 1 to 9, if **period_type** is set to **month**. • The value ranges from 1 to 3, if **period_type** is set to **year**.
resource_package_type	Yes	Array of strings	Specifies the dedicated package.

Parameter	Mandatory	Type	Description
auto_pay	No	Boolean	Specifies whether an order is automatically paid using your account balance without manual operations. Constraints: If you use automatic payment, only your account balance can be used. If you want to use a voucher, disable automatic payment and select the voucher for the payment in the Billing Center. Value options: • **true**: Enable automatic payment. • **false**: Disable automatic payment.

Response Parameters

Status code: 202

Table 5-68 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
job_id	String	Specifies the upgrade task ID.

Example Requests

Example: Upgrading a shared load balancer with **action** set to **start**

```
POST https://{ELB_Endpoint}/v3/060576798a80d5762fafc01a9b5eedc7/elb/loadbalancers/
2c0b5b97-221b-4136-afc2-15d6570f31cb/upgrade

{
  "action" : "start",
  "availability_zone_list" : [ "AZ1" ],
  "elb_virsubnet_ids" : [ "5eddff5a-f45f-46d7-9f2b-70dc669feff9" ],
  "l4_flavor_id" : "f3c46bc2-1304-40b4-902b-cefae3858d17",
  "l7_flavor_id" : "1b333094-bd31-4cb8-97e2-ea762fde3576"
}
```

Example Responses

Status code: 202

The request has been received and is being processed.

```
{
  "request_id" : "841e0da7-5835-4130-9a47-01688f34a154",
  "job_id" : "062804a2-9e39-4dde-bd9b-271859ee312b"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Example: Upgrading a shared load balancer with **action** set to **start**

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;

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

public class UpgradeLoadbalancerSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        UpgradeLoadbalancerRequest request = new UpgradeLoadbalancerRequest();
        request.withLoadbalancerId("{loadbalancer_id}");
        UpgradeV3RequestBody body = new UpgradeV3RequestBody();
        List<String> listbodyElbVirsubnetIds = new ArrayList<>();
        listbodyElbVirsubnetIds.add("5eddff5a-f45f-46d7-9f2b-70dc669feff9");
        List<String> listbodyAvailabilityZoneList = new ArrayList<>();
        listbodyAvailabilityZoneList.add("AZ1");
        body.withElbVirsubnetIds(listbodyElbVirsubnetIds);
        body.withAvailabilityZoneList(listbodyAvailabilityZoneList);
        body.withL7FlavorId("1b333094-bd31-4cb8-97e2-ea762fde3576");
        body.withL4FlavorId("f3c46bc2-1304-40b4-902b-cefae3858d17");
        body.withAction(UpgradeV3RequestBody.ActionEnum.fromValue("start"));
        request.withBody(body);
        try {
            UpgradeLoadbalancerResponse response = client.upgradeLoadbalancer(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

Example: Upgrading a shared load balancer with **action** set to **start**

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpgradeLoadbalancerRequest()
        request.loadbalancer_id = "{loadbalancer_id}"
        listElbVirsubnetIdsbody = [
            "5eddff5a-f45f-46d7-9f2b-70dc669feff9"
        ]
        listAvailabilityZoneListbody = [
            "AZ1"
        ]
        request.body = UpgradeV3RequestBody(
            elb_virsubnet_ids=listElbVirsubnetIdsbody,
            availability_zone_list=listAvailabilityZoneListbody,
            l7_flavor_id="1b333094-bd31-4cb8-97e2-ea762fde3576",
            l4_flavor_id="f3c46bc2-1304-40b4-902b-cefae3858d17",
            action="start"
        )
        response = client.upgrade_loadbalancer(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

Example: Upgrading a shared load balancer with **action** set to **start**

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpgradeLoadbalancerRequest{}
    request.LoadbalancerId = "{loadbalancer_id}"
    var listElbVirsubnetIdsbody = []string{
        "5eddff5a-f45f-46d7-9f2b-70dc669feff9",
    }
    var listAvailabilityZoneListbody = []string{
        "AZ1",
    }
    l7FlavorIdUpgradeV3RequestBody:= "1b333094-bd31-4cb8-97e2-ea762fde3576"
    l4FlavorIdUpgradeV3RequestBody:= "f3c46bc2-1304-40b4-902b-cefae3858d17"
    request.Body = &model.UpgradeV3RequestBody{
        ElbVirsubnetIds: &listElbVirsubnetIdsbody,
        AvailabilityZoneList: &listAvailabilityZoneListbody,
        L7FlavorId: &l7FlavorIdUpgradeV3RequestBody,
        L4FlavorId: &l4FlavorIdUpgradeV3RequestBody,
        Action: model.GetUpgradeV3RequestBodyActionEnum().START,
    }
    response, err := client.UpgradeLoadbalancer(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
202	The request has been received and is being processed.

Error Codes

See **Error Codes**.

5.6.4 Querying Load Balancers

Function

This API is used to query all load balancers.

Constraints

This API has the following constraints:

- Parameters **marker**, **limit**, and **page_reverse** are used for pagination query.
- Parameters **marker** and **page_reverse** take effect only when they are used together with parameter **limit**.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/loadbalancers

Table 5-69 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID of the load balancer.

Table 5-70 Query Parameters

Parameter	Mandatory	Type	Description
marker	No	String	Specifies the ID of the last record on the previous page. Note: • This parameter must be used together with **limit**. • If this parameter is not specified, the first page will be queried. • This parameter cannot be left blank or set to an invalid ID.
limit	No	Integer	Specifies the number of records on each page. Value range: 0–2000 Default value: 2000
page_reverse	No	Boolean	Specifies whether to use reverse query. Value options: • **true**: Query the previous page. • **false** (default): Query the next page. Note: • This parameter must be used together with **limit**. • If **page_reverse** is set to **true** and you want to query the previous page, set the value of **marker** to the value of **previous_marker**.
id	No	Array of strings	Specifies the load balancer ID. Multiple IDs can be queried in the format of *id=xxx&id=xxx*.
name	No	Array of strings	Specifies the load balancer name. Multiple names can be queried in the format of *name=xxx&name=xxx*.

Parameter	Mandatory	Type	Description
description	No	Array of strings	Provides supplementary information about the load balancer. Multiple descriptions can be queried in the format of *description=xxx&description=xxx*.
admin_state_up	No	Boolean	Specifies whether the load balancer is enabled. Value options: • **true**: indicates the load balancer is enabled. • **false**: indicates the load balancer is disabled.
provisioning_status	No	Array of strings	Specifies the provisioning status of the load balancer. • **ACTIVE**: The load balancer is successfully provisioned. • **PENDING_DELETE**: The load balancer is being deleted. Multiple provisioning statuses can be queried in the format of *provisioning_status=xxx&provisioning_status=xxx*.
operating_status	No	Array of strings	Specifies the operating status of the load balancer. • **ONLINE**: The load balancer is working normally. • **FROZEN**: The load balancer has been frozen. Multiple operating statuses can be queried in the format of *operating_status=xxx&operating_status=xxx*.
guaranteed	No	Boolean	Specifies whether the load balancer is a dedicated load balancer. • **false**: The load balancer is a shared load balancer. • **true**: The load balancer is a dedicated load balancer.

Parameter	Mandatory	Type	Description
vpc_id	No	Array of strings	Specifies the ID of the VPC where the load balancer resides. Multiple IDs can be queried in the format of *vpc_id=xxx&vpc_id=xxx*.
vip_port_id	No	Array of strings	Specifies the ID of the port bound to the private IPv4 address of the load balancer. Multiple IDs can be queried in the format of *vip_port_id=xxx&vip_port_id=xxx*.
vip_address	No	Array of strings	Specifies the private IPv4 address bound to the load balancer. Multiple virtual IP addresses can be queried in the format of *vip_address=xxx&vip_address=xxx*.
vip_subnet_cidr_id	No	Array of strings	Specifies the ID of the IPv4 subnet where the load balancer resides. Multiple IDs can be queried in the format of *vip_subnet_cidr_id=xxx&vip_subnet_cidr_id=xxx*.
ipv6_vip_port_id	No	Array of strings	Specifies the ID of the port bound to the IPv6 address of the load balancer. Multiple ports can be queried in the format of *ipv6_vip_port_id=xxx&ipv6_vip_port_id=xxx*.
ipv6_vip_address	No	Array of strings	Specifies the IPv6 address bound to the load balancer. Multiple IPv6 addresses can be queried in the format of *ipv6_vip_address=xxx&ipv6_vip_address=xxx*.

Parameter	Mandatory	Type	Description
ipv6_vip_virsubnet_id	No	Array of strings	Specifies the ID of the IPv6 subnet where the load balancer resides. Multiple IDs can be queried in the format of *ipv6_vip_virsubnet_id=xxx&ipv6_vip_virsubnet_id=xxx*.

Parameter	Mandatory	Type	Description

eips	No	Array of strings	Specifies the IPv4 EIP bound to the load balancer. The following is an example:
			"eips": [
			{
			"eip_id": "e9b72a9d-4275-455e-a724-853504e4d9c6",
			"eip_address": "88.88.14.122",
			"ip_version": 4
			}
			]
			If you want to query the load balancers that have the above EIP bound, you can use the format of eips=ip_version%3D4&eips=eip_address%3D88.88.14.122&eips=eip_id%3De9b72a9d-4275-455e-a724-853504e4d9c6.
			Multiple EIPs can be queried.
			• If **eip_id** is used as the query condition, the format is *eips=eip_id=xxx&eips=eip_id=xxx*.
			• If **eip_address** is used as the query condition, the format is *eips=eip_address=xxx&eips=eip_address=xxx*.
			• If **ip_version** is used as the query condition, the format is *eips=ip_version=xxx&eips=ip_version=xxx*.
			Note that this parameter has the same meaning as **publicips**.

Parameter	Mandatory	Type	Description

publicips	No	Array of strings	Specifies the IPv4 EIP bound to the load balancer. The following is an example:
			"publicips": [
			{
			"publicip_id": "e9b72a9d-4275-455e-a724-853504e4d9c6",
			"publicip_address": "88.88.14.122",
			"ip_version": 4
			}
			]
			You can use **publicips=ip_version%3D4&publicips=public_address%3D88.88.14.122&publicips=public_id%3De9b72a9d-4275-455e-a724-853504e4d9c6** to query the load balancers that have the above EIP bound.
			Multiple EIPs can be queried.
			• If **publicip_id** is used as the query condition, the format is *publicips=publicip_id=xxx&publicips=publicip_id=xxx*.
			• If **publicip_address** is used as the query condition, the format is *publicips=publicip_address=xxx&publicips=publicip_address=xxx*.
			• If **publicip_address** is used as the query condition, the format is *publicips=ip_version=xxx&publicips=ip_version=xxx*.
			Note that this parameter has the same meaning as **eips**.

Parameter	Mandatory	Type	Description
availability_zone_list	No	Array of strings	Specifies the list of AZs where the load balancer is created. Multiple AZs can be queried in the format of *availability_zone_list=xxx&availability_zone_list=xxx*.
l4_flavor_id	No	Array of strings	Specifies the ID of a flavor at Layer 4. Multiple IDs can be queried in the format of *l4_flavor_id=xxx&l4_flavor_id=xxx*.
l4_scale_flavor_id	No	Array of strings	Specifies the ID of the elastic flavor at Layer 4, which is reserved for now. Multiple flavors can be queried in the format of *l4_scale_flavor_id=xxx&l4_scale_flavor_id=xxx*. This parameter is unsupported. Please do not use it.
l7_flavor_id	No	Array of strings	Specifies the ID of a flavor at Layer 7. Multiple flavors can be queried in the format of *l7_flavor_id=xxx&l7_flavor_id=xxx*.
l7_scale_flavor_id	No	Array of strings	Specifies the ID of the elastic flavor at Layer 7. Multiple flavors can be queried in the format of *l7_scale_flavor_id=xxx&l7_scale_flavor_id=xxx*. This parameter is unsupported. Please do not use it.

Parameter	Mandatory	Type	Description
billing_info	No	Array of strings	Provides resource billing information. Multiple values can be queried in the format of *billing_info=xxx&billing_info=xxx*. This parameter is unsupported. Please do not use it.
member_device_id	No	Array of strings	Specifies the ID of the cloud server that is associated with the load balancer as a backend server. This is a query parameter and will not be included in the response. Multiple IDs can be queried in the format of *member_device_id=xxx&member_device_id=xxx*.
member_address	No	Array of strings	Specifies the private IP address of the cloud server that is associated with the load balancer as a backend server. This is a query parameter and will not be included in the response. Multiple private IP addresses can be queried in the format of *member_address=xxx&member_address=xxx*.

Parameter	Mandatory	Type	Description
enterprise_project_id	No	Array of strings	Specifies the ID of the enterprise project. • If **enterprise_project_id** is not specified, resources in all enterprise projects are queried by default. Fine-grained authorization is performed. The **elb:loadbalancers:list** permission must be assigned to the user group. • If **enterprise_project_id** is specified, the value can be a specific enterprise project ID or **all_granted_eps**. If the value is a specific enterprise project ID, only resources in the enterprise project are queried. If the value is **all_granted_eps**, resources in the enterprise projects with the **elb:loadbalancers:list** permission are queried. Multiple values can be queried in the format of *enterprise_project_id=xxx&enterprise_project_id=xxx*.
ip_version	No	Array of integers	Specifies the IP version. The value can be **4** (IPv4) or **6** (IPv6). Multiple versions can be queried in the format of *ip_version=xxx&ip_version=xxx*.
deletion_protection_enable	No	Boolean	Specifies whether to enable deletion protection. Value options: • **true**: Enable deletion protection. • **false** (default): Disable deletion protection.

Parameter	Mandatory	Type	Description
elb_virsubnet_type	No	Array of strings	Specifies the type of the subnet on the downstream plane. • **ipv4**: IPv4 subnet • **dualstack**: subnet that supports IPv4/IPv6 dual stack Multiple values can be queried in the format of *elb_virsubnet_type=ipv4&elb_virsubnet_type=dualstack*.

autoscaling	No	Array of strings	Specifies whether to enable elastic scaling. Example:
			"autoscaling": {
			"enable": "true"
			}
			Multiple values can be queried in the format of *autoscaling=enable=true&autoscaling=enable=false*.

protection_status	No	Array of strings	Specifies the protection status. Value options: • **nonProtection** (default): The load balancer is not protected. • **consoleProtection**: **Modification Protection** is enabled on the console.

Parameter	Mandatory	Type	Description

global_eips	No	Array of strings	Specifies the EIP bound to the load balancer. The following shows an example:
			{
			"global_eips": [
			{
			"global_eip_id": "24000000-0000-0000-0000-100000000001",
			"global_eip_address": "10.10.10.10",
			"ip_version": 4
			}
			]
			}
			EIPs can be queried by different conditions.
			• If **global_eip_id** is used as the query condition, the format is *global_eips=global_eip_id=xxx&global_eips=global_eip_id=xxx*.
			• If **global_eip_address** is used as the query condition, the format is *global_eips=global_eip_address=xxx&global_eips=global_eip_address=xxx*.
			• If **ip_version** is used as the query condition, the format is *global_eips=ip_version=xxx&global_eips=ip_version=xxx*.

log_topic_id	No	String	Specifies the ID of the log group that is associated with the load balancer. Multiple IDs can be queried in the format of *log_topic_id=xxx&log_topic_id=xxx*.

Parameter	Mandatory	Type	Description
log_group_id	No	String	Specifies the ID of the log topic that is associated with the load balancer. Multiple IDs can be queried in the format of *log_group_id=xxx&log_group_id=xxx*.

Request Parameters

Table 5-71 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-72 Response body parameters

Parameter	Type	Description
loadbalancers	Array of **LoadBalancer** objects	Lists the load balancers.
page_info	**PageInfo** object	Shows pagination information about load balancers.
request_id	String	Specifies the request ID. Note: The value is automatically generated.

Table 5-73 LoadBalancer

Parameter	Type	Description
id	String	Specifies the load balancer ID.
description	String	Provides supplementary information about the load balancer.

Parameter	Type	Description
provisioning_status	String	Specifies the provisioning status of the load balancer. Value options: • **ACTIVE**: The load balancer is successfully provisioned. • **PENDING_DELETE**: The load balancer is being deleted.
admin_state_up	Boolean	Specifies whether the load balancer is enabled. Value options: • **true**: indicates the load balancer is enabled. • **false**: indicates the load balancer is disabled.
provider	String	Specifies the provider of the load balancer. The value can only be **vlb**.
pools	Array of **PoolRef** objects	Lists the IDs of backend server groups associated with the load balancer.
listeners	Array of **ListenerRef** objects	Lists the IDs of listeners added to the load balancer.
operating_status	String	Specifies the operating status of the load balancer. Value options: • **ONLINE**: indicates that the load balancer is running normally. • **FROZEN**: indicates that the load balancer is frozen.
name	String	Specifies the load balancer name.
project_id	String	Specifies the project ID of the load balancer.
vip_subnet_cidr_id	String	Specifies the ID of the frontend IPv4 subnet where the load balancer resides.
vip_address	String	Specifies the private IPv4 address bound to the load balancer.
vip_port_id	String	Specifies the ID of the port bound to the private IPv4 address of the load balancer.

Parameter	Type	Description
tags	Array of **Tag** objects	Lists the tags added to the load balancer.
created_at	String	Specifies the time when the load balancer was created, in the format of *yyyy-MM-dd''T''HH:mm:ss''Z''*.
updated_at	String	Specifies the time when the load balancer was updated, in the format of *yyyy-MM-dd''T''HH:mm:ss''Z''*.
guaranteed	Boolean	Specifies whether the load balancer is a dedicated load balancer. Value options: • **true** (default): The load balancer is a dedicated load balancer. • **false**: The load balancer is a shared load balancer.
vpc_id	String	Specifies the ID of the VPC where the load balancer resides.
eips	Array of **EipInfo** objects	Specifies the EIP bound to the load balancer. Only one EIP can be bound to a load balancer. This parameter has the same meaning as **publicips**.
ipv6_vip_address	String	Specifies the IPv6 address bound to the load balancer.
ipv6_vip_virsubnet_id	String	Specifies the ID of the IPv6 subnet where the load balancer resides.
ipv6_vip_port_id	String	Specifies the ID of the port bound to the IPv6 address of the load balancer.
availability_zone_list	Array of strings	Specifies the list of AZs where the load balancer is created.
enterprise_project_id	String	Specifies the enterprise project ID. If this parameter is not passed during resource creation, **"0"** will be returned, and the resource belongs to the default enterprise project. Note: **"0"** is not a valid enterprise project ID and cannot be used in the APIs for creating, updating the load balancer, or querying the details of the load balancer.

Parameter	Type	Description
billing_info	String	Provides resource billing information. • If the value is left blank, the resource is billed in pay-per-use mode. This parameter is unsupported. Please do not use it.
l4_flavor_id	String	Specifies the ID of a flavor at Layer 4. **l4_flavor_id** defines the maximum elastic flavor at Layer 4. Note: • If **l4_flavor_id** is specified, the load balancer is billed by fixed specifications. • If **L4_elastic_max** is specified, the load balancer is billed by how many LCUs you use.
l4_scale_flavor_id	String	Specifies the ID of the reserved flavor at Layer 4. This parameter is unsupported. Please do not use it.
l7_flavor_id	String	Specifies the ID of a flavor at Layer 7. **l7_flavor_id** defines the maximum elastic flavor at Layer 7. Note: • If **l7_flavor_id** is specified, the load balancer is billed by fixed specifications. • If **L7_elastic_max** is specified, the load balancer is billed by how many LCUs you use.
l7_scale_flavor_id	String	Specifies the ID of the reserved flavor at Layer 7. This parameter is unsupported. Please do not use it.
publicips	Array of **PublicIpInfo** objects	Specifies the EIP bound to the load balancer. Only one EIP can be bound to a load balancer. This parameter has the same meaning as **eips**.

Parameter	Type	Description
global_eips	Array of **GlobalEipInfo** objects	Specifies the global EIP bound to the load balancer. Only the first global EIP specified under **global_eips** will be bound.
elb_virsubnet_ids	Array of strings	Lists the IDs of subnets on the downstream plane.
elb_virsubnet_type	String	Specifies the type of the subnet on the downstream plane. Value options: • **ipv4**: IPv4 subnet • **dualstack**: subnet that supports IPv4/IPv6 dual stack
ip_target_enable	Boolean	Specifies whether to add backend servers that are not in the load balancer's VPC. If you enable this function, you can add servers in a peer VPC connected through a VPC peering connection, servers in other public clouds, or servers in an on-premises data center at the other end of a Direct Connect or VPN connection, by using their IP addresses. Value options: • **true**: Enable **IP as a Backend**. • **false**: Disable **IP as a Backend**. Note: • The value can only be updated to **true**. • If you need to connect your server to a shared VPC, ensure the VPC principal has created a VPC peering connections between the two VPCs. • This function is supported only by dedicated load balancers.

Parameter	Type	Description
frozen_scene	String	Specifies the scenario where the load balancer is frozen. Multiple values are separated using commas (,). Value options: • **POLICE**: The load balancer is frozen due to security reasons. • **ILLEGAL**: The load balancer is frozen due to violation of laws and regulations. • **VERIFY**: Your account has not completed real-name authentication. • **PARTNER**: The load balancer is frozen by the partner. • **ARREAR**: Your account is in arrears.
ipv6_bandwidth	**BandwidthRef** object	Specifies the ID of the bandwidth used by an IPv6 address. Note: This parameter is available only when you create or update a load balancer with a public IPv6 address. If you use a new IPv6 address and specify a shared bandwidth, the IPv6 address will be added to the shared bandwidth.
deletion_protection_enable	Boolean	Specifies whether to enable deletion protection. Value options: • **true**: Enable deletion protection. • **false**: Disable deletion protection. Note: • Disable deletion protection for all your resources before deleting your account. • This parameter is returned only when deletion protection is enabled at the site.

Parameter	Type	Description
autoscaling	**AutoscalingRef** object	Specifies information about elastic scaling. If elastic scaling is enabled, the load balancer specifications can be automatically adjusted based on incoming traffic. Note: • This parameter is only available for users on the whitelist. • If elastic scaling is enabled, **l4_flavor_id** indicates the ID of the maximum elastic flavor at Layer 4. **l7_flavor_id** indicates the ID of the maximum elastic flavor at Layer 7. • This parameter has been deprecated, but is retained for compatibility purposes. Using this parameter is not recommended. If this parameter is specified, the load balancer with minimum specifications will be created and you will be billed for the minimum specifications.
public_border_group	String	Specifies the AZ group to which the load balancer belongs.
charge_mode	String	Specifies the charge mode when creating a load balancer. Value options: • **flavor**: billed by the fixed specification you select. • **lcu**: billed by how many LCUs you have used. • If this parameter is left blank: – If it is a shared load balancer, it is free. – If it is a dedicated load balancer, it will be billed by the fixed specification you select.

Parameter	Type	Description
waf_failure_action	String	Specifies traffic distributing policies when the WAF is faulty. Value options: • **discard**: Traffic will not be distributed. • **forward** (default): Traffic will be distributed to the default backend servers. Note: This parameter takes effect only when WAF is enabled for the load balancer.
protection_status	String	Specifies the protection status. Value options: • **nonProtection** (default): The load balancer is not protected. • **consoleProtection**: **Modification Protection** is enabled on the console.
protection_reason	String	Specifies why the modification protection is enabled. Note: This parameter is valid only when **protection_status** is set to **consoleProtection**. The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).
log_group_id	String	Specifies the ID of the log group that is associated with the load balancer.
log_topic_id	String	Specifies the ID of the log topic that is associated with the load balancer.

Table 5-74 PoolRef

Parameter	Type	Description
id	String	Specifies the ID of the backend server group.

Table 5-75 ListenerRef

Parameter	Type	Description
id	String	Specifies the listener ID.

Table 5-76 Tag

Parameter	Type	Description
key	String	Specifies the tag key.
value	String	Specifies the tag value.

Table 5-77 EipInfo

Parameter	Type	Description
eip_id	String	Specifies the EIP ID.
eip_address	String	Specifies the EIP.
ip_version	Integer	Specifies the IP version. **4** indicates IPv4, and **6** indicates IPv6.

Table 5-78 PublicIpInfo

Parameter	Type	Description
publicip_id	String	Specifies the EIP ID.
publicip_address	String	Specifies the IP address.
ip_version	Integer	Specifies the IP version. The value can be **4** (IPv4) or **6** (IPv6).

Table 5-79 GlobalEipInfo

Parameter	Type	Description
global_eip_id	String	Specifies the ID of the global EIP.
global_eip_address	String	Specifies the global EIP.

Parameter	Type	Description
ip_version	Integer	Specifies the IP version. The value can be **4** and **6**. **4** indicates an IPv4 address, and **6** indicates an IPv6 address.

Table 5-80 BandwidthRef

Parameter	Type	Description
id	String	Specifies the shared bandwidth ID.

Table 5-81 AutoscalingRef

Parameter	Type	Description
enable	Boolean	Specifies whether to enable elastic scaling for the load balancer. Value options: • **true**: Enable elastic scaling. • **false** (default): Disable elastic scaling.
min_l7_flavor_id	String	Specifies the ID of the minimum elastic flavor at Layer 7. Note: • This parameter cannot be left blank if there are HTTP or HTTPS listeners. • This parameter has been deprecated, but is retained for compatibility purposes. Using this parameter is not recommended. If this parameter is specified, the load balancer with minimum specifications will be created and you will be billed for the minimum specifications.

Table 5-82 PageInfo

Parameter	Type	Description
previous_marker	String	Specifies the ID of the first record in the pagination query result. When **page_reverse** is set to **true**, this parameter is used together to query resources on the previous page.
next_marker	String	Specifies the ID of the last record in the pagination query result.
current_count	Integer	Specifies the number of records.

Example Requests

- Querying load balancers on each page

  ```
  GET https://{ELB_Endpoint}/v3/b2782e6708b8475c993e6064bc456bf8/elb/loadbalancers?limit=2&marker=87627cb6-9ff1-4580-984f-cc564fa9fc34
  ```

- Querying load balancers using multiple IDs

  ```
  GET https://{ELB_Endpoint}/v3/b2782e6708b8475c993e6064bc456bf8/elb/loadbalancers?id=87627cb6-9ff1-4580-984f-cc564fa9fc34&id=09e86f09-03fc-440e-8132-03f3e149e979
  ```

Example Responses

Status code: 200

Successful request.


```
{
  "request_id" : "46b7d911-cece-408c-a2cc-55c78ab025d8",
  "loadbalancers" : [ {
    "id" : "65672f7e-2024-4c39-9198-98249da479c5",
    "project_id" : "057ef081eb00d2732fd1c01a9be75e6f",
    "name" : "dxq_2021_07_26_11_12_37",
    "description" : "",
    "vip_port_id" : "b289f890-a6fa-4405-a9cc-fe62b8a3bed0",
    "vip_address" : "172.16.0.152",
    "admin_state_up" : true,
    "provisioning_status" : "ACTIVE",
    "operating_status" : "ONLINE",
    "listeners" : [ {
      "id" : "dc9572eb-a5b2-47b3-a982-44892d833892"
    } ],
    "pools" : [ {
      "id" : "dc6b01c4-f704-4427-a4c2-21cd5f58d177"
    } ],
    "tags" : [ ],
    "provider" : "vlb",
    "created_at" : "2021-07-26T03:12:37Z",
    "updated_at" : "2021-07-26T03:12:37Z",
    "vpc_id" : "6e0ee31f-7a46-4530-b32f-ce41f30959d4",
    "enterprise_project_id" : "0",
    "availability_zone_list" : [ "az1" ],
    "ipv6_vip_address" : "2001:db8:a583:4cb:d6b8:f8b4:4211:fe72",
    "ipv6_vip_virsubnet_id" : "0b9e3c5e-3ec8-46b3-bab9-80b1450e59ee",
    "ipv6_vip_port_id" : "5186bb47-24e5-4171-b795-62d22846db9b",
    "publicips" : [ ],
    "elb_virsubnet_ids" : [ "0b9e3c5e-3ec8-46b3-bab9-80b1450e59ee" ],
    "elb_virsubnet_type" : "dualstack",
```



```
  "ip_target_enable" : false,
  "autoscaling" : {
    "enable" : false,
    "min_l7_flavor_id" : ""
  },
  "frozen_scene" : null,
  "eips" : [ ],
  "guaranteed" : true,
  "billing_info" : null,
  "l4_flavor_id" : "aa06b26b-9ff9-43c6-92b9-41e0f746bca6",
  "l4_scale_flavor_id" : null,
  "l7_flavor_id" : "e2a5675c-a181-444e-b9a5-17b052dc7fb9",
  "l7_scale_flavor_id" : null,
  "vip_subnet_cidr_id" : "96e52038-7983-462f-8a96-415d8a280b13",
  "public_border_group" : "center",
  "log_topic_id" : null,
  "log_group_id" : null
}, {
  "id" : "cce5318e-c79a-4f68-94a2-9fb285c6efbe",
  "project_id" : "057ef081eb00d2732fd1c01a9be75e6f",
  "name" : "elb-reset",
  "description" : "",
  "vip_port_id" : null,
  "vip_address" : null,
  "admin_state_up" : true,
  "provisioning_status" : "ACTIVE",
  "operating_status" : "ONLINE",
  "listeners" : [ {
    "id" : "0ae21c37-8b90-4e73-8a35-eedde6d2538c"
  } ],
  "pools" : [ {
    "id" : "904ecca6-8ebb-4974-9c5c-61d1d66fba17"
  } ],
  "tags" : [ ],
  "provider" : "vlb",
  "created_at" : "2021-07-26T02:46:31Z",
  "updated_at" : "2021-07-26T02:46:59Z",
  "vpc_id" : "59cb11ef-f185-49ba-92af-0539e8ff9734",
  "enterprise_project_id" : "0",
  "availability_zone_list" : [ "az1" ],
  "ipv6_vip_address" : null,
  "ipv6_vip_virsubnet_id" : null,
  "ipv6_vip_port_id" : null,
  "publicips" : [ {
    "publicip_id" : "0c07e04d-e2f9-41ad-b934-f58a65b6734d",
    "publicip_address" : "97.97.2.171",
    "ip_version" : 4
  } ],
  "elb_virsubnet_ids" : [ "7f817f9c-8731-4002-9e47-18cb8d431787" ],
  "elb_virsubnet_type" : "dualstack",
  "ip_target_enable" : false,
  "autoscaling" : {
    "enable" : false,
    "min_l7_flavor_id" : ""
  },
  "frozen_scene" : null,
  "eips" : [ {
    "eip_id" : "0c07e04d-e2f9-41ad-b934-f58a65b6734d",
    "eip_address" : "97.97.2.171",
    "ip_version" : 4
  } ],
  "guaranteed" : true,
  "billing_info" : null,
  "l4_flavor_id" : "636ba721-935a-4ca5-a685-8076ce0e4148",
  "l4_scale_flavor_id" : null,
  "l7_flavor_id" : null,
  "l7_scale_flavor_id" : null,
  "vip_subnet_cidr_id" : null,
  "public_border_group" : "center",
```



```
    "log_topic_id" : null,
    "log_group_id" : null
  } ],
  "page_info" : {
    "next_marker" : "cce5318e-c79a-4f68-94a2-9fb285c6efbe",
    "previous_marker" : "65672f7e-2024-4c39-9198-98249da479c5",
    "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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ListLoadBalancersSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ListLoadBalancersRequest request = new ListLoadBalancersRequest();
        try {
            ListLoadBalancersResponse response = client.listLoadBalancers(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListLoadBalancersRequest()
        response = client.list_load_balancers(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
```



```
        Build())

    request := &model.ListLoadBalancersRequest{}
    response, err := client.ListLoadBalancers(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	Successful request.

Error Codes

See **Error Codes**.

5.6.5 Copying a Load Balancer

Function

This API is used to copy a load balancer.

Calling Method

For details, see **Calling APIs**.

URI

POST /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}/clone

Table 5-83 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the ID of the project where the load balancer is used.
loadbalancer_id	Yes	String	Specifies the load balancer ID.

Request Parameters

Table 5-84 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Table 5-85 Request body parameters

Parameter	Mandatory	Type	Description
count	No	Integer	Specifies the maximum number of replicas at a time. Value range: 1 to 10 Default value: 1
target_loadbalancer_param	Yes	**TargetLoadbalancerParam** object	Specifies the parameters for the new load balancer.

Table 5-86 TargetLoadbalancerParam

Parameter	Mandatory	Type	Description
name	No	String	(Optional) Specifies the new load balancer name. If this parameter is not specified, the new load balancer name will be the original load balancer name plus suffix **copy-x**.
availability_zone_list	No	Array of strings	(Optional) Specifies the AZ where new load balancer works. If this parameter is not specified, the AZ of the original load balancer is used. This parameter is available only for copying a dedicated load balancer.

Parameter	Mandatory	Type	Description
vip_subnet_cidr_id	No	String	(Optional) Specifies the ID of the IPv4 subnet where the new load balancer works. If this parameter is not specified, the IPv4 subnet of the original load balancer is used. The subnets where the original and new load balancers work must be in the same VPC.
vip_address	No	String	(Optional) Specifies the private IPv4 address of the new load balancer. If this parameter is not specified, a private IPv4 address will be randomly assigned to the new load balancer. This parameter is available only when you copy a dedicated or shared load balancer as a dedicated load balancer.
ipv6_vip_virsubnet_id	No	String	(Optional) Specifies the ID of the IPv6 subnet where the new load balancer works. If this parameter is not specified, the IPv6 subnet of the original load balancer is used. The subnets where the original and new load balancers work must be in the same VPC. This parameter is available only for copying a dedicated load balancer.

Parameter	Mandatory	Type	Description
ipv6_vip_address	No	String	(Optional) Specifies the private IPv6 address of the new load balancer. If this parameter is not specified, a private IPv6 address will be randomly assigned to the new load balancer. This parameter is available only for copying a dedicated load balancer.
elb_virsubnet_ids	No	Array of strings	(Optional) Specifies the ID of the backend subnet of the new load balancer. If this parameter is not specified, the backend subnet of the original load balancer is used. The subnets where the original and new load balancers work must be in the same VPC. This parameter is available only when you copy a dedicated or shared load balancer as a dedicated load balancer.
l4_flavor_id	No	String	(Optional) Specifies the Layer 4 specifications of the new load balancer. If this parameter is not specified, the Layer 4 specifications of the original load balancer are used. This parameter is available only when you copy a dedicated or shared load balancer as a dedicated load balancer.

Parameter	Mandatory	Type	Description
l7_flavor_id	No	String	(Optional) Specifies the Layer 7 specifications of the new load balancer. If this parameter is not specified, the Layer 7 specifications of the original load balancer are used. This parameter is available only when you copy a dedicated or shared load balancer as a dedicated load balancer.
enterprise_project_id	No	String	(Optional) Specifies the enterprise project where the new load balancer is used. If this parameter is not specified, the enterprise project of the original load balancer is used.
reuse_pool	No	Boolean	(Optional) Specifies whether to reuse the backend server group and backend server ID of the original load balancer. If this parameter is set to **true**, the backend server group of the original load balancer will be used. If no backend server group is selected, a new backend server group is created by default. This parameter is invalid when **enterprise_project_id** is set to another enterprise project. This parameter is available only when you copy a dedicated or shared load balancer as a dedicated load balancer.

Parameter	Mandatory	Type	Description
guaranteed	No	Boolean	(Optional) Specifies the type of the new load balancer. When a dedicated load balancer is copied, the default value is **true**. If the value is explicitly specified, it can only be set to **true**. When a shared load balancer is copied, the default value is **false**. If the value is explicitly set to **false**, the new load balancer is a shared load balancer. If the value is explicitly set to **true**, the new load balancer is a dedicated load balancer.

Response Parameters

Status code: 200

Table 5-87 Response body parameters

Parameter	Type	Description
loadbalancer_list	Array of **loadbalancer_list** objects	Specifies the information about the new load balancer.
request_id	String	Specifies the request ID.
job_id	String	Specifies the copy task ID.

Table 5-88 loadbalancer_list

Parameter	Type	Description
id	String	Specifies the ID of the new load balancer.

Example Requests

Copying a load balancer

```
POST https://{ELB_Endpoint}/v3/{project_id}/elb/loadbalancers/{loadbalancer_id}/clone

{
```



```
  "target_loadbalancer_param" : {
    "availability_zone_list" : [ "az1", "az2" ],
    "vip_address" : "1.1.1.1",
    "guaranteed" : true
  }
}
```

Example Responses

Status code: 200

Normal response

```
{
  "loadbalancer_list" : [ {
    "id" : "00ac869a-16f2-4335-b40a-15f277604f18"
  } ],
  "request_id" : "53013c36-751b-4687-9819-cc0bb609468c",
  "job_id" : "3ccae6c1-615c-48b4-82b5-abfcdcb82849"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Copying a load balancer

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;

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

public class CloneLoadbalancerSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        CloneLoadbalancerRequest request = new CloneLoadbalancerRequest();
        request.withLoadbalancerId("{loadbalancer_id}");
```



```
        CloneLoadbalancerRequestBody body = new CloneLoadbalancerRequestBody();
        List<String> listTargetLoadbalancerParamAvailabilityZoneList = new ArrayList<>();
        listTargetLoadbalancerParamAvailabilityZoneList.add("az1");
        listTargetLoadbalancerParamAvailabilityZoneList.add("az2");
        TargetLoadbalancerParam targetLoadbalancerParambody = new TargetLoadbalancerParam();

targetLoadbalancerParambody.withAvailabilityZoneList(listTargetLoadbalancerParamAvailabilityZoneList)
            .withVipAddress("1.1.1.1")
            .withGuaranteed(true);
        body.withTargetLoadbalancerParam(targetLoadbalancerParambody);
        request.withBody(body);
        try {
            CloneLoadbalancerResponse response = client.cloneLoadbalancer(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

Copying a load balancer

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CloneLoadbalancerRequest()
        request.loadbalancer_id = "{loadbalancer_id}"
        listAvailabilityZoneListTargetLoadbalancerParam = [
            "az1",
            "az2"
        ]
        targetLoadbalancerParambody = TargetLoadbalancerParam(
            availability_zone_list=listAvailabilityZoneListTargetLoadbalancerParam,
            vip_address="1.1.1.1",
            guaranteed=True
        )
```



```
        request.body = CloneLoadbalancerRequestBody(
            target_loadbalancer_param=targetLoadbalancerParambody
        )
        response = client.clone_loadbalancer(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

Copying a load balancer

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CloneLoadbalancerRequest{}
    request.LoadbalancerId = "{loadbalancer_id}"
    var listAvailabilityZoneListTargetLoadbalancerParam = []string{
        "az1",
        "az2",
    }
    vipAddressTargetLoadbalancerParam:= "1.1.1.1"
    guaranteedTargetLoadbalancerParam:= true
    targetLoadbalancerParambody := &model.TargetLoadbalancerParam{
        AvailabilityZoneList: &listAvailabilityZoneListTargetLoadbalancerParam,
        VipAddress: &vipAddressTargetLoadbalancerParam,
        Guaranteed: &guaranteedTargetLoadbalancerParam,
    }
    request.Body = &model.CloneLoadbalancerRequestBody{
        TargetLoadbalancerParam: targetLoadbalancerParambody,
    }
    response, err := client.CloneLoadbalancer(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

Error Codes

See **Error Codes**.

5.6.6 Viewing the Details of a Load Balancer

Function

This API is used to view the details of a load balancer.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}

Table 5-89 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
loadbalancer_id	Yes	String	Specifies the load balancer ID.

Request Parameters

Table 5-90 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-91 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
loadbalancer	**LoadBalancer** object	Specifies the load balancer.

Table 5-92 LoadBalancer

Parameter	Type	Description
id	String	Specifies the load balancer ID.
description	String	Provides supplementary information about the load balancer.
provisioning_status	String	Specifies the provisioning status of the load balancer. Value options: • **ACTIVE**: The load balancer is successfully provisioned. • **PENDING_DELETE**: The load balancer is being deleted.
admin_state_up	Boolean	Specifies whether the load balancer is enabled. Value options: • **true**: indicates the load balancer is enabled. • **false**: indicates the load balancer is disabled.

Parameter	Type	Description
provider	String	Specifies the provider of the load balancer. The value can only be **vlb**.
pools	Array of **PoolRef** objects	Lists the IDs of backend server groups associated with the load balancer.
listeners	Array of **ListenerRef** objects	Lists the IDs of listeners added to the load balancer.
operating_status	String	Specifies the operating status of the load balancer. Value options: • **ONLINE**: indicates that the load balancer is running normally. • **FROZEN**: indicates that the load balancer is frozen.
name	String	Specifies the load balancer name.
project_id	String	Specifies the project ID of the load balancer.
vip_subnet_cidr_id	String	Specifies the ID of the frontend IPv4 subnet where the load balancer resides.
vip_address	String	Specifies the private IPv4 address bound to the load balancer.
vip_port_id	String	Specifies the ID of the port bound to the private IPv4 address of the load balancer.
tags	Array of **Tag** objects	Lists the tags added to the load balancer.
created_at	String	Specifies the time when the load balancer was created, in the format of *yyyy-MM-dd''T''HH:mm:ss''Z''*.
updated_at	String	Specifies the time when the load balancer was updated, in the format of *yyyy-MM-dd''T''HH:mm:ss''Z''*.
guaranteed	Boolean	Specifies whether the load balancer is a dedicated load balancer. Value options: • **true** (default): The load balancer is a dedicated load balancer. • **false**: The load balancer is a shared load balancer.

Parameter	Type	Description
vpc_id	String	Specifies the ID of the VPC where the load balancer resides.
eips	Array of **EipInfo** objects	Specifies the EIP bound to the load balancer. Only one EIP can be bound to a load balancer. This parameter has the same meaning as **publicips**.
ipv6_vip_address	String	Specifies the IPv6 address bound to the load balancer.
ipv6_vip_virsubnet_id	String	Specifies the ID of the IPv6 subnet where the load balancer resides.
ipv6_vip_port_id	String	Specifies the ID of the port bound to the IPv6 address of the load balancer.
availability_zone_list	Array of strings	Specifies the list of AZs where the load balancer is created.
enterprise_project_id	String	Specifies the enterprise project ID. If this parameter is not passed during resource creation, **"0"** will be returned, and the resource belongs to the default enterprise project. Note: **"0"** is not a valid enterprise project ID and cannot be used in the APIs for creating, updating the load balancer, or querying the details of the load balancer.
billing_info	String	Provides resource billing information. • If the value is left blank, the resource is billed in pay-per-use mode. This parameter is unsupported. Please do not use it.
l4_flavor_id	String	Specifies the ID of a flavor at Layer 4. **l4_flavor_id** defines the maximum elastic flavor at Layer 4. Note: • If **l4_flavor_id** is specified, the load balancer is billed by fixed specifications. • If **L4_elastic_max** is specified, the load balancer is billed by how many LCUs you use.

Parameter	Type	Description
l4_scale_flavor_id	String	Specifies the ID of the reserved flavor at Layer 4. This parameter is unsupported. Please do not use it.
l7_flavor_id	String	Specifies the ID of a flavor at Layer 7. **l7_flavor_id** defines the maximum elastic flavor at Layer 7. Note: • If **l7_flavor_id** is specified, the load balancer is billed by fixed specifications. • If **L7_elastic_max** is specified, the load balancer is billed by how many LCUs you use.
l7_scale_flavor_id	String	Specifies the ID of the reserved flavor at Layer 7. This parameter is unsupported. Please do not use it.
publicips	Array of **PublicIpInfo** objects	Specifies the EIP bound to the load balancer. Only one EIP can be bound to a load balancer. This parameter has the same meaning as **eips**.
global_eips	Array of **GlobalEipInfo** objects	Specifies the global EIP bound to the load balancer. Only the first global EIP specified under **global_eips** will be bound.
elb_virsubnet_ids	Array of strings	Lists the IDs of subnets on the downstream plane.
elb_virsubnet_type	String	Specifies the type of the subnet on the downstream plane. Value options: • **ipv4**: IPv4 subnet • **dualstack**: subnet that supports IPv4/IPv6 dual stack

Parameter	Type	Description
ip_target_enable	Boolean	Specifies whether to add backend servers that are not in the load balancer's VPC. If you enable this function, you can add servers in a peer VPC connected through a VPC peering connection, servers in other public clouds, or servers in an on-premises data center at the other end of a Direct Connect or VPN connection, by using their IP addresses. Value options: ● **true**: Enable **IP as a Backend**. ● **false**: Disable **IP as a Backend**. Note: ● The value can only be updated to **true**. ● If you need to connect your server to a shared VPC, ensure the VPC principal has created a VPC peering connections between the two VPCs. ● This function is supported only by dedicated load balancers.
frozen_scene	String	Specifies the scenario where the load balancer is frozen. Multiple values are separated using commas (,). Value options: ● **POLICE**: The load balancer is frozen due to security reasons. ● **ILLEGAL**: The load balancer is frozen due to violation of laws and regulations. ● **VERIFY**: Your account has not completed real-name authentication. ● **PARTNER**: The load balancer is frozen by the partner. ● **ARREAR**: Your account is in arrears.

Parameter	Type	Description
ipv6_bandwidth	**BandwidthRef** object	Specifies the ID of the bandwidth used by an IPv6 address. Note: This parameter is available only when you create or update a load balancer with a public IPv6 address. If you use a new IPv6 address and specify a shared bandwidth, the IPv6 address will be added to the shared bandwidth.
deletion_protection_enable	Boolean	Specifies whether to enable deletion protection. Value options: • **true**: Enable deletion protection. • **false**: Disable deletion protection. Note: • Disable deletion protection for all your resources before deleting your account. • This parameter is returned only when deletion protection is enabled at the site.
autoscaling	**AutoscalingRef** object	Specifies information about elastic scaling. If elastic scaling is enabled, the load balancer specifications can be automatically adjusted based on incoming traffic. Note: • This parameter is only available for users on the whitelist. • If elastic scaling is enabled, **l4_flavor_id** indicates the ID of the maximum elastic flavor at Layer 4. **l7_flavor_id** indicates the ID of the maximum elastic flavor at Layer 7. • This parameter has been deprecated, but is retained for compatibility purposes. Using this parameter is not recommended. If this parameter is specified, the load balancer with minimum specifications will be created and you will be billed for the minimum specifications.
public_border_group	String	Specifies the AZ group to which the load balancer belongs.

Parameter	Type	Description
charge_mode	String	Specifies the charge mode when creating a load balancer. Value options: • **flavor**: billed by the fixed specification you select. • **lcu**: billed by how many LCUs you have used. • If this parameter is left blank: – If it is a shared load balancer, it is free. – If it is a dedicated load balancer, it will be billed by the fixed specification you select.
waf_failure_action	String	Specifies traffic distributing policies when the WAF is faulty. Value options: • **discard**: Traffic will not be distributed. • **forward** (default): Traffic will be distributed to the default backend servers. Note: This parameter takes effect only when WAF is enabled for the load balancer.
protection_status	String	Specifies the protection status. Value options: • **nonProtection** (default): The load balancer is not protected. • **consoleProtection**: **Modification Protection** is enabled on the console.
protection_reason	String	Specifies why the modification protection is enabled. Note: This parameter is valid only when **protection_status** is set to **consoleProtection**. The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).
log_group_id	String	Specifies the ID of the log group that is associated with the load balancer.
log_topic_id	String	Specifies the ID of the log topic that is associated with the load balancer.

Table 5-93 PoolRef

Parameter	Type	Description
id	String	Specifies the ID of the backend server group.

Table 5-94 ListenerRef

Parameter	Type	Description
id	String	Specifies the listener ID.

Table 5-95 Tag

Parameter	Type	Description
key	String	Specifies the tag key.
value	String	Specifies the tag value.

Table 5-96 EipInfo

Parameter	Type	Description
eip_id	String	Specifies the EIP ID.
eip_address	String	Specifies the EIP.
ip_version	Integer	Specifies the IP version. **4** indicates IPv4, and **6** indicates IPv6.

Table 5-97 PublicIpInfo

Parameter	Type	Description
publicip_id	String	Specifies the EIP ID.
publicip_address	String	Specifies the IP address.
ip_version	Integer	Specifies the IP version. The value can be **4** (IPv4) or **6** (IPv6).

Table 5-98 GlobalEipInfo

Parameter	Type	Description
global_eip_id	String	Specifies the ID of the global EIP.
global_eip_address	String	Specifies the global EIP.
ip_version	Integer	Specifies the IP version. The value can be **4** and **6**. **4** indicates an IPv4 address, and **6** indicates an IPv6 address.

Table 5-99 BandwidthRef

Parameter	Type	Description
id	String	Specifies the shared bandwidth ID.

Table 5-100 AutoscalingRef

Parameter	Type	Description
enable	Boolean	Specifies whether to enable elastic scaling for the load balancer. Value options: • **true**: Enable elastic scaling. • **false** (default): Disable elastic scaling.
min_l7_flavor_id	String	Specifies the ID of the minimum elastic flavor at Layer 7. Note: • This parameter cannot be left blank if there are HTTP or HTTPS listeners. • This parameter has been deprecated, but is retained for compatibility purposes. Using this parameter is not recommended. If this parameter is specified, the load balancer with minimum specifications will be created and you will be billed for the minimum specifications.

Example Requests

Querying the details of a given load balancer

```
GET https://{ELB_Endpoint}/v3/060576782980d5762f9ec014dd2f1148/elb/loadbalancers/3dbde7e5-c277-4ea3-a424-edd339357eff
```

Example Responses

Status code: 200

Successful request.


```
{
  "loadbalancer" : {
    "id" : "3dbde7e5-c277-4ea3-a424-edd339357eff",
    "project_id" : "060576782980d5762f9ec014dd2f1148",
    "name" : "elb-l4-no-delete",
    "description" : null,
    "vip_port_id" : "f079c7ee-65a9-44ef-be86-53d8927e59be",
    "vip_address" : "10.0.0.196",
    "admin_state_up" : true,
    "provisioning_status" : "ACTIVE",
    "operating_status" : "ONLINE",
    "listeners" : [ ],
    "pools" : [ {
      "id" : "1d864dc9-f6ef-4366-b59d-7034cde2328f"
    }, {
      "id" : "c0a2e4a1-c028-4a24-a62f-e721c52f5513"
    }, {
      "id" : "79308896-6169-4c28-acbc-e139eb661996"
    } ],
    "tags" : [ ],
    "provider" : null,
    "created_at" : "2019-12-02T09:55:11Z",
    "updated_at" : "2019-12-02T09:55:11Z",
    "vpc_id" : "70711260-9de9-4d96-9839-0ae698e00109",
    "enterprise_project_id" : "0",
    "availability_zone_list" : [ ],
    "ipv6_vip_address" : null,
    "ipv6_vip_virsubnet_id" : null,
    "ipv6_vip_port_id" : null,
    "publicips" : [ ],
    "elb_virsubnet_ids" : [ "ad5d63bf-3b50-4e88-b4d9-e94a59aade48" ],
    "eips" : [ ],
    "guaranteed" : true,
    "billing_info" : null,
    "l4_flavor_id" : "e5acacda-f861-404e-9871-df480c49d185",
    "l4_scale_flavor_id" : null,
    "l7_flavor_id" : null,
    "l7_scale_flavor_id" : null,
    "vip_subnet_cidr_id" : "396d918a-756e-4163-8450-3bdc860109cf",
    "deletion_protection_enable" : false,
    "autoscaling" : {
      "enable" : true,
      "min_l7_flavor_id" : "0c8cf29d-51cb-4c1d-8e25-1c61cf5c2b00"
    },
    "public_border_group" : "center"
  },
  "request_id" : "1a47cfbf-969f-4e40-8c0e-c2e60b14bcac"
}
```


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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ShowLoadBalancerSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowLoadBalancerRequest request = new ShowLoadBalancerRequest();
        request.withLoadbalancerId("{loadbalancer_id}");
        try {
            ShowLoadBalancerResponse response = client.showLoadBalancer(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowLoadBalancerRequest()
        request.loadbalancer_id = "{loadbalancer_id}"
        response = client.show_load_balancer(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowLoadBalancerRequest{}
    request.LoadbalancerId = "{loadbalancer_id}"
    response, err := client.ShowLoadBalancer(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	Successful request.

Error Codes

See **Error Codes**.

5.6.7 Updating a Load Balancer

Function

This API is used to update a load balancer.

Calling Method

For details, see **Calling APIs**.

URI

PUT /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}

Table 5-101 Path Parameters

Parameter	Mandatory	Type	Description
loadbalancer_id	Yes	String	Specifies the load balancer ID.
project_id	Yes	String	Specifies the project ID.

Request Parameters

Table 5-102 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Table 5-103 Request body parameters

Parameter	Mandatory	Type	Description
loadbalancer	Yes	**UpdateLoadBalancerOption** object	Specifies the load balancer.

Table 5-104 UpdateLoadBalancerOption

Parameter	Mandatory	Type	Description
name	No	String	Specifies the load balancer name.
admin_state_up	No	Boolean	Specifies whether the load balancer is enabled. Value options: • **true**: indicates the load balancer is enabled. • **false**: indicates the load balancer is disabled.
description	No	String	Provides supplementary information about the load balancer.

Parameter	Mandatory	Type	Description
ipv6_vip_virsubnet_id	No	String	Specifies the ID of the IPv6 subnet where the load balancer resides. You can query parameter **neutron_network_id** in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets). Note: • The IPv6 subnet can be updated using **ipv6_vip_virsubnet_id**, and the private IPv6 address of the load balancer will be changed accordingly. • This parameter will be passed only when IPv6 is enabled for the subnet. The subnet specified by **ipv6_vip_virsubnet_id** must be in the VPC specified by **vpc_id**. • This parameter can be updated only when **guaranteed** is set to **true**. • The value will become **null** if the IPv6 address is unbound from the load balancer. • The IPv4 subnet will not change, if IPv6 subnet is updated.

Parameter	Mandatory	Type	Description
vip_subnet_cidr_id	No	String	Specifies the ID of the IPv4 subnet where the load balancer resides. You can query parameter **neutron_subnet_id** in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets). Note: • The IPv4 subnet can be updated using **vip_subnet_cidr_id**, and the private IPv4 address of the load balancer will be changed accordingly. • If **vip_address** is also specified, the IP address specified by **vip_address** must be in the subnet specified by **vip_subnet_cidr_id** and will be used as the private IPv4 address of the load balancer. • The IPv4 subnet must be in the VPC where the load balancer resides. • This parameter can be updated only when **guaranteed** is set to **true**. • The value will become **null** if the private IPv4 address is unbound from the load balancer. • The IPv6 subnet will not change, if IPv4 subnet is updated.

Parameter	Mandatory	Type	Description
vip_address	No	String	Specifies the private IPv4 address bound to the load balancer. Note: • The IP address must be from the IPv4 subnet where the load balancer resides and should not be occupied by other services. • **vip_address** can be updated only when **guaranteed** is set to **true**.
l4_flavor_id	No	String	Specifies the ID of a flavor at Layer 4. Note: • You can query parameter **id** in the response by calling the API (GET https://{ELB_Endpoint}/v3/{project_id}/elb/flavors?type=L4). • This parameter can be updated only when **guaranteed** is set to **true**. • If you change the flavor, you can select a higher or lower one. If you select a lower one, part of persistent connections will be interrupted. • If **autoscaling.enable** is set to **true**, changes to this parameter will not take effect. • If the specification type is **L4**, the load balancer uses the fixed specifications and will be billed by the specification you select. • If the specification type is **L4_elastic_max**, the load balancer uses the elastic specifications and will be billed by how many LCUs you use.

Parameter	Mandatory	Type	Description
l7_flavor_id	No	String	Specifies the ID of a flavor at Layer 7. Note: • You can query parameter **id** in the response by calling the API (GET https://{ELB_Endpoint}/v3/{project_id}/elb/flavors?type=L7). • This parameter can be updated only when **guaranteed** is set to **true**. • If you change the flavor, you can select a higher or lower one. If you select a lower one, part of persistent connections will be interrupted. • If **autoscaling.enable** is set to **true**, changes to this parameter will not take effect. • If the specification type is **L7**, the load balancer uses the fixed specifications and will be billed by the specification you select. • If the specification type is **L7_elastic_max**, the load balancer uses the elastic specifications and will be billed by how many LCUs you use.
ipv6_bandwidth	No	**BandwidthRef** object	Specifies the ID of the bandwidth used by an IPv6 address. Note: This parameter is available only when you create or update a load balancer with a public IPv6 address. If you use a new IPv6 address and specify a shared bandwidth, the IPv6 address will be added to the shared bandwidth.

Parameter	Mandatory	Type	Description
ip_target_enable	No	Boolean	Specifies whether to add backend servers that are not in the load balancer's VPC. If you enable this function, you can add servers in a peer VPC connected through a VPC peering connection, servers in other public clouds, or servers in an on-premises data center at the other end of a Direct Connect or VPN connection, by using their IP addresses. Value options: • **true**: Enable **IP as a Backend**. • **false**: Disable **IP as a Backend**. Note: • The value can only be updated to **true**. • If you need to connect your server to a shared VPC, ensure the VPC principal has created a VPC peering connections between the two VPCs. • This function is supported only by dedicated load balancers.

Parameter	Mandatory	Type	Description
elb_virsubnet_ids	No	Array of strings	Specifies the IDs of subnets on the downstream plane. You can query parameter **neutron_network_id** in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets). Note: • If the IDs of the subnets required by the load balancer are specified in **elb_virsubnet_ids**, the subnets will still be bound to the load balancer. • If the IDs of the subnets are specified in **elb_virsubnet_ids**, but not on the downstream plane, a new load balancer will be bound to the downstream plane. • If the IDs of the subnets required by the load balancer are not specified in **elb_virsubnet_ids**, the subnets will be unbound from the load balancers. Do not unbind the subnets that have been used by the load balancer. Otherwise, an error will be returned. • All subnets belong to the same VPC where the load balancer resides. • Edge subnets are not supported.

Parameter	Mandatory	Type	Description
deletion_protection_enable	No	Boolean	Specifies whether to enable deletion protection. Value options: • **true**: Enable deletion protection. • **false**: Disable deletion protection. **NOTE** Disable deletion protection for all your resources before deleting your account.
prepaid_options	No	**PrepaidUpdateOption** object	Updates the yearly/monthly billing information during the change of load balancer flavors. This parameter is unsupported. Please do not use it.
autoscaling	No	**UpdateLoadbalancerAutoscalingOption** object	Specifies information about elastic scaling. If elastic scaling is enabled, the load balancer specifications can be automatically adjusted based on incoming traffic. Note: • This parameter is only available for users on the whitelist. • If elastic scaling is enabled, **l4_flavor_id** indicates the ID of the maximum elastic flavor at Layer 4. **l7_flavor_id** indicates the ID of the maximum elastic flavor at Layer 7. • This parameter has been deprecated, but is retained for compatibility purposes. Using this parameter is not recommended. If this parameter is specified, the load balancer with minimum specifications will be created and you will be billed for the minimum specifications.

Parameter	Mandatory	Type	Description
charge_mode	No	String	Specifies the charge mode when updating a load balancer. Value options: • **flavor**: billed by the specifications you will select.
waf_failure_action	No	String	Specifies traffic distributing policies when the WAF is faulty. Value options: • **discard**: Traffic will not be distributed. • **forward** (default): Traffic will be distributed to the default backend servers. Note: This parameter takes effect only when WAF is enabled for the load balancer.
protection_status	No	String	Specifies the protection status. Value options: • **nonProtection**: The load balancer is not protected. • **consoleProtection**: **Modification Protection** is enabled on the console.
protection_reason	No	String	Specifies why the modification protection is enabled. Note: This parameter is valid only when **protection_status** is set to **consoleProtection**. The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).
ipv6_vip_address	No	String	Specifies the IPv6 address bound to the load balancer.

Table 5-105 BandwidthRef

Parameter	Mandatory	Type	Description
id	Yes	String	Specifies the shared bandwidth ID.

Table 5-106 PrepaidUpdateOption

Parameter	Mandatory	Type	Description
auto_pay	No	Boolean	Specifies whether the payment will be automatically deducted from the customer's account after an order is placed. • **true**: The payment will be automatically deducted from the customer's account. • **false** (default): The payment will not be automatically deducted from the customer's account. If you want to use coupons, submit your request. The system automatically will switch to the billing center, where you can use the coupons.
change_mode	No	String	Specifies the flavor change type. Value options: • **immediate** (default) indicates that the change takes effect immediately. • **delay** indicates that the change takes effect after the current period ends.

Parameter	Mandatory	Type	Description
period_num	No	Integer	Specifies the number of subscription periods. The value varies with the operation policy, and the default value is **1**. This parameter takes effect only when **change_mode** is set to **delay**. • If **period_type** is set to **month**, the value ranges from **1** to **9**. • If **period_type** is set to **year**, the value ranges from **1** to **3**.
period_type	No	String	Specifies the subscription period type. Yearly/Monthly subscription is supported. This parameter takes effect only when **change_mode** is set to **delay**. • **month** (default): monthly subscription • **year**: yearly subscription

Table 5-107 UpdateLoadbalancerAutoscalingOption

Parameter	Mandatory	Type	Description
enable	Yes	Boolean	Specifies whether to enable elastic scaling the load balancer. Value options: • **true**: Enable elastic scaling. • **false**: Disable elastic scaling.

Parameter	Mandatory	Type	Description
min_l7_flavor_id	No	String	Specifies the ID of the minimum elastic flavor at Layer 7. Note: • This parameter cannot be left blank if there are Layer 7 listeners. • This parameter has been deprecated, but is retained for compatibility purposes. Using this parameter is not recommended. If this parameter is specified, the load balancer with minimum specifications will be created and you will be billed for the minimum specifications.

Response Parameters

Status code: 200

Table 5-108 Response body parameters

Parameter	Type	Description
loadbalancer	**LoadBalancer** object	Specifies the load balancer.
request_id	String	Specifies the request ID. Note: The value is automatically generated.

Table 5-109 LoadBalancer

Parameter	Type	Description
id	String	Specifies the load balancer ID.
description	String	Provides supplementary information about the load balancer.

Parameter	Type	Description
provisioning_status	String	Specifies the provisioning status of the load balancer. Value options: • **ACTIVE**: The load balancer is successfully provisioned. • **PENDING_DELETE**: The load balancer is being deleted.
admin_state_up	Boolean	Specifies whether the load balancer is enabled. Value options: • **true**: indicates the load balancer is enabled. • **false**: indicates the load balancer is disabled.
provider	String	Specifies the provider of the load balancer. The value can only be **vlb**.
pools	Array of **PoolRef** objects	Lists the IDs of backend server groups associated with the load balancer.
listeners	Array of **ListenerRef** objects	Lists the IDs of listeners added to the load balancer.
operating_status	String	Specifies the operating status of the load balancer. Value options: • **ONLINE**: indicates that the load balancer is running normally. • **FROZEN**: indicates that the load balancer is frozen.
name	String	Specifies the load balancer name.
project_id	String	Specifies the project ID of the load balancer.
vip_subnet_cidr_id	String	Specifies the ID of the frontend IPv4 subnet where the load balancer resides.
vip_address	String	Specifies the private IPv4 address bound to the load balancer.
vip_port_id	String	Specifies the ID of the port bound to the private IPv4 address of the load balancer.

Parameter	Type	Description
tags	Array of **Tag** objects	Lists the tags added to the load balancer.
created_at	String	Specifies the time when the load balancer was created, in the format of *yyyy-MM-dd''T''HH:mm:ss''Z''*.
updated_at	String	Specifies the time when the load balancer was updated, in the format of *yyyy-MM-dd''T''HH:mm:ss''Z''*.
guaranteed	Boolean	Specifies whether the load balancer is a dedicated load balancer. Value options: • **true** (default): The load balancer is a dedicated load balancer. • **false**: The load balancer is a shared load balancer.
vpc_id	String	Specifies the ID of the VPC where the load balancer resides.
eips	Array of **EipInfo** objects	Specifies the EIP bound to the load balancer. Only one EIP can be bound to a load balancer. This parameter has the same meaning as **publicips**.
ipv6_vip_address	String	Specifies the IPv6 address bound to the load balancer.
ipv6_vip_virsubnet_id	String	Specifies the ID of the IPv6 subnet where the load balancer resides.
ipv6_vip_port_id	String	Specifies the ID of the port bound to the IPv6 address of the load balancer.
availability_zone_list	Array of strings	Specifies the list of AZs where the load balancer is created.
enterprise_project_id	String	Specifies the enterprise project ID. If this parameter is not passed during resource creation, **"0"** will be returned, and the resource belongs to the default enterprise project. Note: **"0"** is not a valid enterprise project ID and cannot be used in the APIs for creating, updating the load balancer, or querying the details of the load balancer.

Parameter	Type	Description
billing_info	String	Provides resource billing information. • If the value is left blank, the resource is billed in pay-per-use mode. This parameter is unsupported. Please do not use it.
l4_flavor_id	String	Specifies the ID of a flavor at Layer 4. **l4_flavor_id** defines the maximum elastic flavor at Layer 4. Note: • If **l4_flavor_id** is specified, the load balancer is billed by fixed specifications. • If **L4_elastic_max** is specified, the load balancer is billed by how many LCUs you use.
l4_scale_flavor_id	String	Specifies the ID of the reserved flavor at Layer 4. This parameter is unsupported. Please do not use it.
l7_flavor_id	String	Specifies the ID of a flavor at Layer 7. **l7_flavor_id** defines the maximum elastic flavor at Layer 7. Note: • If **l7_flavor_id** is specified, the load balancer is billed by fixed specifications. • If **L7_elastic_max** is specified, the load balancer is billed by how many LCUs you use.
l7_scale_flavor_id	String	Specifies the ID of the reserved flavor at Layer 7. This parameter is unsupported. Please do not use it.
publicips	Array of **PublicIpInfo** objects	Specifies the EIP bound to the load balancer. Only one EIP can be bound to a load balancer. This parameter has the same meaning as **eips**.

Parameter	Type	Description
global_eips	Array of **GlobalEipInfo** objects	Specifies the global EIP bound to the load balancer. Only the first global EIP specified under **global_eips** will be bound.
elb_virsubnet_ids	Array of strings	Lists the IDs of subnets on the downstream plane.
elb_virsubnet_type	String	Specifies the type of the subnet on the downstream plane. Value options: • **ipv4**: IPv4 subnet • **dualstack**: subnet that supports IPv4/IPv6 dual stack
ip_target_enable	Boolean	Specifies whether to add backend servers that are not in the load balancer's VPC. If you enable this function, you can add servers in a peer VPC connected through a VPC peering connection, servers in other public clouds, or servers in an on-premises data center at the other end of a Direct Connect or VPN connection, by using their IP addresses. Value options: • **true**: Enable **IP as a Backend**. • **false**: Disable **IP as a Backend**. Note: • The value can only be updated to **true**. • If you need to connect your server to a shared VPC, ensure the VPC principal has created a VPC peering connections between the two VPCs. • This function is supported only by dedicated load balancers.

Parameter	Type	Description
frozen_scene	String	Specifies the scenario where the load balancer is frozen. Multiple values are separated using commas (,). Value options: • **POLICE**: The load balancer is frozen due to security reasons. • **ILLEGAL**: The load balancer is frozen due to violation of laws and regulations. • **VERIFY**: Your account has not completed real-name authentication. • **PARTNER**: The load balancer is frozen by the partner. • **ARREAR**: Your account is in arrears.
ipv6_bandwidth	**BandwidthRef** object	Specifies the ID of the bandwidth used by an IPv6 address. Note: This parameter is available only when you create or update a load balancer with a public IPv6 address. If you use a new IPv6 address and specify a shared bandwidth, the IPv6 address will be added to the shared bandwidth.
deletion_protection_enable	Boolean	Specifies whether to enable deletion protection. Value options: • **true**: Enable deletion protection. • **false**: Disable deletion protection. Note: • Disable deletion protection for all your resources before deleting your account. • This parameter is returned only when deletion protection is enabled at the site.

Parameter	Type	Description
autoscaling	**AutoscalingRef** object	Specifies information about elastic scaling. If elastic scaling is enabled, the load balancer specifications can be automatically adjusted based on incoming traffic. Note: • This parameter is only available for users on the whitelist. • If elastic scaling is enabled, **l4_flavor_id** indicates the ID of the maximum elastic flavor at Layer 4. **l7_flavor_id** indicates the ID of the maximum elastic flavor at Layer 7. • This parameter has been deprecated, but is retained for compatibility purposes. Using this parameter is not recommended. If this parameter is specified, the load balancer with minimum specifications will be created and you will be billed for the minimum specifications.
public_border_group	String	Specifies the AZ group to which the load balancer belongs.
charge_mode	String	Specifies the charge mode when creating a load balancer. Value options: • **flavor**: billed by the fixed specification you select. • **lcu**: billed by how many LCUs you have used. • If this parameter is left blank: – If it is a shared load balancer, it is free. – If it is a dedicated load balancer, it will be billed by the fixed specification you select.

Parameter	Type	Description
waf_failure_action	String	Specifies traffic distributing policies when the WAF is faulty. Value options: • **discard**: Traffic will not be distributed. • **forward** (default): Traffic will be distributed to the default backend servers. Note: This parameter takes effect only when WAF is enabled for the load balancer.
protection_status	String	Specifies the protection status. Value options: • **nonProtection** (default): The load balancer is not protected. • **consoleProtection**: **Modification Protection** is enabled on the console.
protection_reason	String	Specifies why the modification protection is enabled. Note: This parameter is valid only when **protection_status** is set to **consoleProtection**. The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).
log_group_id	String	Specifies the ID of the log group that is associated with the load balancer.
log_topic_id	String	Specifies the ID of the log topic that is associated with the load balancer.

Table 5-110 PoolRef

Parameter	Type	Description
id	String	Specifies the ID of the backend server group.

Table 5-111 ListenerRef

Parameter	Type	Description
id	String	Specifies the listener ID.

Table 5-112 Tag

Parameter	Type	Description
key	String	Specifies the tag key.
value	String	Specifies the tag value.

Table 5-113 EipInfo

Parameter	Type	Description
eip_id	String	Specifies the EIP ID.
eip_address	String	Specifies the EIP.
ip_version	Integer	Specifies the IP version. **4** indicates IPv4, and **6** indicates IPv6.

Table 5-114 PublicIpInfo

Parameter	Type	Description
publicip_id	String	Specifies the EIP ID.
publicip_address	String	Specifies the IP address.
ip_version	Integer	Specifies the IP version. The value can be **4** (IPv4) or **6** (IPv6).

Table 5-115 GlobalEipInfo

Parameter	Type	Description
global_eip_id	String	Specifies the ID of the global EIP.
global_eip_address	String	Specifies the global EIP.

Parameter	Type	Description
ip_version	Integer	Specifies the IP version. The value can be **4** and **6**. **4** indicates an IPv4 address, and **6** indicates an IPv6 address.

Table 5-116 BandwidthRef

Parameter	Type	Description
id	String	Specifies the shared bandwidth ID.

Table 5-117 AutoscalingRef

Parameter	Type	Description
enable	Boolean	Specifies whether to enable elastic scaling for the load balancer. Value options: • **true**: Enable elastic scaling. • **false** (default): Disable elastic scaling.
min_l7_flavor_id	String	Specifies the ID of the minimum elastic flavor at Layer 7. Note: • This parameter cannot be left blank if there are HTTP or HTTPS listeners. • This parameter has been deprecated, but is retained for compatibility purposes. Using this parameter is not recommended. If this parameter is specified, the load balancer with minimum specifications will be created and you will be billed for the minimum specifications.

Example Requests

Modifying the description and name of a load balancer

```
PUT https://{ELB_Endpoint}/v3/{project_id}/elb/loadbalancers/{loadbalancer_id}

{
  "loadbalancer" : {
```



```
    "description" : "loadbalancer",
    "name" : "loadbalancer-update"
  }
}
```

Example Responses

Status code: 200

Successful request.

```
{
  "request_id" : "010dad1e-32a3-4405-ab83-62a1fc5f8722",
  "loadbalancer" : {
    "id" : "2e073bf8-edfe-4e51-a699-d915b0b8af89",
    "project_id" : "b2782e6708b8475c993e6064bc456bf8",
    "name" : "loadbalancer-update",
    "description" : "loadbalancer",
    "vip_port_id" : null,
    "vip_address" : null,
    "admin_state_up" : true,
    "provisioning_status" : "ACTIVE",
    "operating_status" : "ONLINE",
    "listeners" : [ {
      "id" : "41937176-bf64-4b58-8e0d-9ff2d0d32c54"
    }, {
      "id" : "abc6ac93-ad0e-4765-bd5a-eec632efde56"
    }, {
      "id" : "b9d8ba97-6d60-467d-838d-f3550b54c22a"
    }, {
      "id" : "fd797ebd-263d-4b18-96e9-e9188d36c69e"
    } ],
    "pools" : [ {
      "id" : "0aabcaa8-c35c-4ddc-a60c-9032d0ac0b80"
    }, {
      "id" : "165d9092-396e-4a8d-b398-067496a447d2"
    } ],
    "tags" : [ ],
    "provider" : "vlb",
    "created_at" : "2019-04-20T03:10:37Z",
    "updated_at" : "2019-05-24T02:11:58Z",
    "vpc_id" : "2037c5bb-e04b-4de2-9300-9051af18e417",
    "enterprise_project_id" : "0",
    "availability_zone_list" : [ "AZ1", "AZ2", "dc3" ],
    "ipv6_vip_address" : null,
    "ipv6_vip_virsubnet_id" : null,
    "ipv6_vip_port_id" : null,
    "eips" : [ ],
    "guaranteed" : true,
    "billing_info" : null,
    "l4_flavor_id" : null,
    "l4_scale_flavor_id" : null,
    "l7_flavor_id" : null,
    "l7_scale_flavor_id" : null,
    "vip_subnet_cidr_id" : null,
    "deletion_protection_enable" : false,
    "public_border_group" : "center"
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Modifying the description and name of a load balancer


```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class UpdateLoadBalancerSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdateLoadBalancerRequest request = new UpdateLoadBalancerRequest();
        request.withLoadbalancerId("{loadbalancer_id}");
        UpdateLoadBalancerRequestBody body = new UpdateLoadBalancerRequestBody();
        UpdateLoadBalancerOption loadbalancerbody = new UpdateLoadBalancerOption();
        loadbalancerbody.withName("loadbalancer-update")
            .withDescription("loadbalancer");
        body.withLoadbalancer(loadbalancerbody);
        request.withBody(body);
        try {
            UpdateLoadBalancerResponse response = client.updateLoadBalancer(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

Modifying the description and name of a load balancer

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdateLoadBalancerRequest()
        request.loadbalancer_id = "{loadbalancer_id}"
        loadbalancerbody = UpdateLoadBalancerOption(
            name="loadbalancer-update",
            description="loadbalancer"
        )
        request.body = UpdateLoadBalancerRequestBody(
            loadbalancer=loadbalancerbody
        )
        response = client.update_load_balancer(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

Modifying the description and name of a load balancer

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
```



```
        WithCredential(auth).
        Build())

    request := &model.UpdateLoadBalancerRequest{}
    request.LoadbalancerId = "{loadbalancer_id}"
    nameLoadbalancer:= "loadbalancer-update"
    descriptionLoadbalancer:= "loadbalancer"
    loadbalancerbody := &model.UpdateLoadBalancerOption{
        Name: &nameLoadbalancer,
        Description: &descriptionLoadbalancer,
    }
    request.Body = &model.UpdateLoadBalancerRequestBody{
        Loadbalancer: loadbalancerbody,
    }
    response, err := client.UpdateLoadBalancer(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	Successful request.

Error Codes

See **Error Codes**.

5.6.8 Deleting a Load Balancer

Function

This API is used to delete a load balancer.

Constraints

All listeners added to the load balancer must be deleted before the load balancer is deleted.

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}

Table 5-118 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
loadbalancer_id	Yes	String	Specifies the load balancer ID.

Request Parameters

Table 5-119 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

None

Example Requests

Deleting a load balancer

```
DELETE https://{ELB_Endpoint}/v3/060576782980d5762f9ec014dd2f1148/elb/loadbalancers/
32c1057f-74a1-42d6-9b20-d55b80ab89c4
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class DeleteLoadBalancerSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteLoadBalancerRequest request = new DeleteLoadBalancerRequest();
        request.withLoadbalancerId("{loadbalancer_id}");
        try {
            DeleteLoadBalancerResponse response = client.deleteLoadBalancer(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteLoadBalancerRequest()
        request.loadbalancer_id = "{loadbalancer_id}"
        response = client.delete_load_balancer(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteLoadBalancerRequest{}
    request.LoadbalancerId = "{loadbalancer_id}"
    response, err := client.DeleteLoadBalancer(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	Successful request.

Error Codes

See **Error Codes**.

5.6.9 Deleting a Load Balancer and Its Associated Resources

Function

This API is used to delete a load balancer and its associated resources, including the listeners, backend server groups, and backend servers.

Note:

- If a load balancer has EIPs bound to it, the EIPs will be unbound from the load balancer.
- Backend server groups are either disassociated from the load balancer if they are associated with other load balancers or deleted if they are not associated with other load balancers.
- When shared load balancers are deleted, their backend server groups will also be deleted.

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}/force-elb

Table 5-120 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the ID of the project where the load balancer is used.
loadbalancer_id	Yes	String	Specifies the load balancer ID.

Request Parameters

Table 5-121 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

None

Example Requests

Deleting a load balancer and resources associated with it

```
DELETE https://{ELB_Endpoint}/v3/060576782980d5762f9ec014dd2f1148/elb/loadbalancers/
32c1057f-74a1-42d6-9b20-d55b80ab89c4/force-elb
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class DeleteLoadBalancerForceSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteLoadBalancerForceRequest request = new DeleteLoadBalancerForceRequest();
        request.withLoadbalancerId("{loadbalancer_id}");
        try {
            DeleteLoadBalancerForceResponse response = client.deleteLoadBalancerForce(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteLoadBalancerForceRequest()
        request.loadbalancer_id = "{loadbalancer_id}"
        response = client.delete_load_balancer_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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteLoadBalancerForceRequest{}
    request.LoadbalancerId = "{loadbalancer_id}"
    response, err := client.DeleteLoadBalancerForce(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 DELETE requests.

Error Codes

See **Error Codes**.

5.6.10 Deleting a Load Balancer and Its Associated Resources (Including EIPs)

Function

This API is used to delete a load balancer and its associated resources, including the listeners, backend server groups, backend servers, and EIPs.

Note: Backend server groups are either disassociated from the load balancer if they are associated with other load balancers or deleted if they are not associated with other load balancers.

Calling Method

For details, see **Calling APIs**.

URI

POST /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}/delete-cascade

Table 5-122 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the ID of the project where the load balancer is used.
loadbalancer_id	Yes	String	Specifies the load balancer ID.

Request Parameters

Table 5-123 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Table 5-124 Request body parameters

Parameter	Mandatory	Type	Description
loadbalancer	Yes	**DeleteLoadBalancerCascadeOption** object	Specifies the load balancer.

Table 5-125 DeleteLoadBalancerCascadeOption

Parameter	Mandatory	Type	Description
unbounded_pool	No	Boolean	Specifies whether to delete the backend server group after it is disassociated from the load balancer. Value options: • **true**: Delete the backend server group. • **false**: Disassociate the backend server group from the load balancer. Default value: **true** Note: • For shared load balancers, the parameter can only be set to **true**. • If this backend server group is associated with other load balancers, the backend server group will not be deleted even if this parameter is set to **true**.
public_ip	No	Boolean	Specifies whether to release EIPs after the load balancer is deleted. Value options: • **true**: Release EIPs. • **false**: Unbind the EIPs from the load balancer.

Response Parameters

None

Example Requests

Deleting a load balancer and its associated resources (including EIPs)

```
POST https://{ELB_Endpoint}/v3/060576782980d5762f9ec014dd2f1148/elb/loadbalancers/
32c1057f-74a1-42d6-9b20-d55b80ab89c4/cascade-delete

{
  "loadbalancer" : {
    "unbounded_pool" : true,
    "public_ip" : true
  }
}
```


Example Responses

None

SDK Sample Code

The SDK sample code is as follows.

Java

Deleting a load balancer and its associated resources (including EIPs)

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class DeleteLoadBalancerCascadeSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteLoadBalancerCascadeRequest request = new DeleteLoadBalancerCascadeRequest();
        request.withLoadbalancerId("{loadbalancer_id}");
        DeleteLoadBalancerCascadeRequestBody body = new DeleteLoadBalancerCascadeRequestBody();
        DeleteLoadBalancerCascadeOption loadbalancerbody = new DeleteLoadBalancerCascadeOption();
        loadbalancerbody.withUnboundedPool(true)
            .withPublicIp(true);
        body.withLoadbalancer(loadbalancerbody);
        request.withBody(body);
        try {
            DeleteLoadBalancerCascadeResponse response = client.deleteLoadBalancerCascade(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

Deleting a load balancer and its associated resources (including EIPs)

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteLoadBalancerCascadeRequest()
        request.loadbalancer_id = "{loadbalancer_id}"
        loadbalancerbody = DeleteLoadBalancerCascadeOption(
            unbounded_pool=True,
            public_ip=True
        )
        request.body = DeleteLoadBalancerCascadeRequestBody(
            loadbalancer=loadbalancerbody
        )
        response = client.delete_load_balancer_cascade(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

Deleting a load balancer and its associated resources (including EIPs)

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteLoadBalancerCascadeRequest{}
    request.LoadbalancerId = "{loadbalancer_id}"
    unboundedPoolLoadbalancer:= true
    publicIpLoadbalancer:= true
    loadbalancerbody := &model.DeleteLoadBalancerCascadeOption{
        UnboundedPool: &unboundedPoolLoadbalancer,
        PublicIp: &publicIpLoadbalancer,
    }
    request.Body = &model.DeleteLoadBalancerCascadeRequestBody{
        Loadbalancer: loadbalancerbody,
    }
    response, err := client.DeleteLoadBalancerCascade(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 DELETE operations.

Error Codes

See **Error Codes**.

5.6.11 Querying the Status Tree of a Load Balancer

Function

This API is used to query the status tree of a load balancer and to show information about all resources associated with the load balancer.

When **admin_state_up** is set to **false** and **operating_status** to **OFFLINE** for a backend server, **DISABLED** is returned for **operating_status** of the backend server in the response of this API.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}/statuses

Table 5-126 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
loadbalancer_id	Yes	String	Specifies the load balancer ID.

Request Parameters

Table 5-127 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-128 Response body parameters

Parameter	Type	Description
statuses	**LoadBalancerStatusResult** object	Provides information about the load balancer status tree.
request_id	String	Specifies the request ID. Note: The value is automatically generated.

Table 5-129 LoadBalancerStatusResult

Parameter	Type	Description
loadbalancer	**LoadBalancerStatus** object	Specifies the statuses of the load balancer and its associated resources.

Table 5-130 LoadBalancerStatus

Parameter	Type	Description
name	String	Specifies the load balancer name.
provisioning_status	String	Specifies the provisioning status of the load balancer. The value can be **ACTIVE** or **PENDING_DELETE**. • **ACTIVE**: The load balancer is successfully provisioned. • **PENDING_DELETE**: The load balancer is being deleted.
listeners	Array of **LoadBalancerStatusListener** objects	Lists the listeners added to the load balancer.
pools	Array of **LoadBalancerStatusPool** objects	Lists the backend server groups associated with the load balancer.
id	String	Specifies the load balancer ID.

Parameter	Type	Description
operating_status	String	Specifies the operating status of the load balancer. The value can only be one of the following: • **ONLINE** (default): The load balancer is running normally. • **FROZEN**: The load balancer has been frozen. • **DEGRADED**: This status is displayed only when **operating_status** is set to **OFFLINE** for a backend server associated with the load balancer and the API for querying the load balancer status tree is called. • **DISABLED**: This status is displayed only when **admin_state_up** of the load balancer is set to **false**. **DEGRADED** and **DISABLED** are returned only when the API for querying the load balancer status tree is called.

Table 5-131 LoadBalancerStatusListener

Parameter	Type	Description
name	String	Specifies the name of the listener added to the load balancer.
provisioning_status	String	Specifies the provisioning status of the listener. The value can only be **ACTIVE**, indicating that the listener is successfully provisioned.
pools	Array of **LoadBalancerStatusPool** objects	Specifies the operating status of the backend server group associated with the listener.
l7policies	Array of **LoadBalancerStatusPolicy** objects	Specifies the operating status of the forwarding policy added to the listener.
id	String	Specifies the listener ID.

Parameter	Type	Description
operating_status	String	Specifies the operating status of the listener. The value can only be one of the following: • **ONLINE** (default): The listener is running normally. • **DEGRADED**: This status is displayed only when **provisioning_status** of a forwarding policy or a forwarding rule added to the listener is set to **ERROR** or **operating_status** is set to **OFFLINE** for a backend server associated with the listener. • **DISABLED**: This status is displayed only when **admin_state_up** of the load balancer or of the listener is set to **false**. Note: **DEGRADED** and **DISABLED** are returned only when the API for querying the load balancer status tree is called.

Table 5-132 LoadBalancerStatusPolicy

Parameter	Type	Description
action	String	Specifies whether requests are forwarded to another backend server group or redirected to an HTTPS listener. Value options: • **REDIRECT_TO_POOL**: Requests are forwarded to another backend server group. • **REDIRECT_TO_LISTENER**: Requests are redirected to an HTTPS listener.
id	String	Specifies the forwarding policy ID.
provisioning_status	String	Specifies the provisioning status of the forwarding policy. • **ACTIVE** (default): The forwarding policy is provisioned successfully. • **ERROR**: Another forwarding policy of the same listener has the same forwarding rule.

Parameter	Type	Description
name	String	Specifies the policy name.
rules	Array of **LoadBalancerStatusL7Rule** objects	Specifies the forwarding rule.

Table 5-133 LoadBalancerStatusL7Rule

Parameter	Type	Description
id	String	Specifies the ID of the forwarding rule.
type	String	Specifies the type of the match content. The value can be **HOST_NAME** or **PATH**. • **HOST_NAME**: A domain name will be used for matching. • **PATH**: A URL will be used for matching. The value must be unique for each forwarding rule in a forwarding policy.
provisioning_status	String	Specifies the provisioning status of the forwarding rule. • **ACTIVE** (default): The forwarding rule is successfully provisioned. • **ERROR**: Another forwarding policy of the same listener has the same forwarding rule.

Table 5-134 LoadBalancerStatusPool

Parameter	Type	Description
provisioning_status	String	Specifies the provisioning status of the backend server group. The value can only be **ACTIVE**, indicating that the backend server group is successfully provisioned.
name	String	Specifies the name of the backend server group.
healthmonitor	**LoadBalancerStatusHealthMonitor** object	Specifies the health check results of backend servers in the load balancer status tree.

Parameter	Type	Description
members	Array of **LoadBalancerStatusMember** objects	Specifies the backend server.
id	String	Specifies the ID of the backend server group.
operating_status	String	Specifies the operating status of the backend server group. Value options: • **ONLINE**: The backend server group is running normally. • **DEGRADED**: This status is displayed only when **operating_status** of a backend server in the backend server group is set to **OFFLINE**. • **DISABLED**: This status is displayed only when **admin_state_up** of the backend server group or of the associated load balancer is set to **false**. Note: **DEGRADED** and **DISABLED** are returned only when the API for querying the load balancer status tree is called.

Table 5-135 LoadBalancerStatusHealthMonitor

Parameter	Type	Description
type	String	Specifies the health check protocol. The value can be **TCP**, **UDP_CONNECT**, or **HTTP**.
id	String	Specifies the health check ID.
name	String	Specifies the health check name.
provisioning_status	String	Specifies the provisioning status of the health check. The value can only be **ACTIVE**, indicating that the health check is successfully provisioned.

Table 5-136 LoadBalancerStatusMember

Parameter	Type	Description
provisioning_status	String	Specifies the provisioning status of the backend server. The value can only be **ACTIVE**, indicating that the backend server is successfully provisioned.
address	String	Specifies the private IP address bound to the backend server.
protocol_port	Integer	Specifies the port used by the backend server to receive requests. The port number ranges from 1 to 65535.
id	String	Specifies the backend server ID.
operating_status	String	Specifies the operating status of the backend server. Value options: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group to which the backend server belongs. • **DISABLED**: The backend server is not available. This status is displayed only when **admin_state_up** of the backend server, or the backend server group to which it belongs, or the associated load balancer is set to **false** and the API for querying the load balancer status tree is called. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist.

Example Requests

Querying the status tree of a load balancer

```
GET https://{ELB_Endpoint}/v3/{project_id}/elb/loadbalancers/38278031-cfca-44be-81be-a412f618773b/statuses
```

Example Responses

Status code: 200

Successful request.


```
{
  "statuses" : {
    "loadbalancer" : {
      "name" : "lb-jy",
      "provisioning_status" : "ACTIVE",
      "listeners" : [ {
        "name" : "listener-jy-1",
        "provisioning_status" : "ACTIVE",
        "pools" : [ {
          "name" : "pool-jy-1",
          "provisioning_status" : "ACTIVE",
          "healthmonitor" : {
            "type" : "TCP",
            "id" : "7422b51a-0ed2-4702-9429-4f88349276c6",
            "name" : "",
            "provisioning_status" : "ACTIVE"
          },
          "members" : [ {
            "protocol_port" : 80,
            "address" : "192.168.44.11",
            "id" : "7bbf7151-0dce-4087-b316-06c7fa17b894",
            "operating_status" : "ONLINE",
            "provisioning_status" : "ACTIVE"
          } ],
          "id" : "c54b3286-2349-4c5c-ade1-e6bb0b26ad18",
          "operating_status" : "ONLINE"
        } ],
        "l7policies" : [ ],
        "id" : "eb84c5b4-9bc5-4bee-939d-3900fb05dc7b",
        "operating_status" : "ONLINE"
      } ],
      "pools" : [ {
        "name" : "pool-jy-1",
        "provisioning_status" : "ACTIVE",
        "healthmonitor" : {
          "type" : "TCP",
          "id" : "7422b51a-0ed2-4702-9429-4f88349276c6",
          "name" : "",
          "provisioning_status" : "ACTIVE"
        },
        "members" : [ {
          "protocol_port" : 80,
          "address" : "192.168.44.11",
          "id" : "7bbf7151-0dce-4087-b316-06c7fa17b894",
          "operating_status" : "ONLINE",
          "provisioning_status" : "ACTIVE"
        } ],
        "id" : "c54b3286-2349-4c5c-ade1-e6bb0b26ad18",
        "operating_status" : "ONLINE"
      } ],
      "id" : "38278031-cfca-44be-81be-a412f618773b",
      "operating_status" : "ONLINE"
    }
  }
}
```


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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ShowLoadBalancerStatusSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowLoadBalancerStatusRequest request = new ShowLoadBalancerStatusRequest();
        request.withLoadbalancerId("{loadbalancer_id}");
        try {
            ShowLoadBalancerStatusResponse response = client.showLoadBalancerStatus(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
```

```
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowLoadBalancerStatusRequest()
        request.loadbalancer_id = "{loadbalancer_id}"
        response = client.show_load_balancer_status(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowLoadBalancerStatusRequest{}
    request.LoadbalancerId = "{loadbalancer_id}"
    response, err := client.ShowLoadBalancerStatus(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	Successful request.

Error Codes

See **Error Codes**.

5.6.12 Deploying a Load Balancer in Other AZs

Function

This API is used to add one or more AZs where a load balancer will work.

Constraints

This API is only available for dedicated load balancers.

Calling Method

For details, see **Calling APIs**.

URI

POST /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}/availability-zone/batch-add

Table 5-137 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the ID of the project where the load balancer is used.
loadbalancer_id	Yes	String	Specifies the load balancer ID.

Request Parameters

Table 5-138 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	Specifies the token used for IAM authentication.

Table 5-139 Request body parameters

Parameter	Mandatory	Type	Description
availability_zone_list	Yes	Array of strings	Specifies the new AZs. This parameter cannot be left blank.

Response Parameters

Status code: 200

Table 5-140 Response body parameters

Parameter	Type	Description
loadbalancer	**LoadBalancer** object	Specifies the load balancer.
request_id	String	Specifies the request ID. Note: The value is automatically generated.

Table 5-141 LoadBalancer

Parameter	Type	Description
id	String	Specifies the load balancer ID.
description	String	Provides supplementary information about the load balancer.
provisioning_status	String	Specifies the provisioning status of the load balancer. Value options: • **ACTIVE**: The load balancer is successfully provisioned. • **PENDING_DELETE**: The load balancer is being deleted.

Parameter	Type	Description
admin_state_up	Boolean	Specifies whether the load balancer is enabled. Value options: • **true**: indicates the load balancer is enabled. • **false**: indicates the load balancer is disabled.
provider	String	Specifies the provider of the load balancer. The value can only be **vlb**.
pools	Array of **PoolRef** objects	Lists the IDs of backend server groups associated with the load balancer.
listeners	Array of **ListenerRef** objects	Lists the IDs of listeners added to the load balancer.
operating_status	String	Specifies the operating status of the load balancer. Value options: • **ONLINE**: indicates that the load balancer is running normally. • **FROZEN**: indicates that the load balancer is frozen.
name	String	Specifies the load balancer name.
project_id	String	Specifies the project ID of the load balancer.
vip_subnet_cidr_id	String	Specifies the ID of the frontend IPv4 subnet where the load balancer resides.
vip_address	String	Specifies the private IPv4 address bound to the load balancer.
vip_port_id	String	Specifies the ID of the port bound to the private IPv4 address of the load balancer.
tags	Array of **Tag** objects	Lists the tags added to the load balancer.
created_at	String	Specifies the time when the load balancer was created, in the format of *yyyy-MM-dd''T''HH:mm:ss''Z''*.
updated_at	String	Specifies the time when the load balancer was updated, in the format of *yyyy-MM-dd''T''HH:mm:ss''Z''*.

Parameter	Type	Description
guaranteed	Boolean	Specifies whether the load balancer is a dedicated load balancer. Value options: • **true** (default): The load balancer is a dedicated load balancer. • **false**: The load balancer is a shared load balancer.
vpc_id	String	Specifies the ID of the VPC where the load balancer resides.
eips	Array of **EipInfo** objects	Specifies the EIP bound to the load balancer. Only one EIP can be bound to a load balancer. This parameter has the same meaning as **publicips**.
ipv6_vip_address	String	Specifies the IPv6 address bound to the load balancer.
ipv6_vip_virsubnet_id	String	Specifies the ID of the IPv6 subnet where the load balancer resides.
ipv6_vip_port_id	String	Specifies the ID of the port bound to the IPv6 address of the load balancer.
availability_zone_list	Array of strings	Specifies the list of AZs where the load balancer is created.
enterprise_project_id	String	Specifies the enterprise project ID. If this parameter is not passed during resource creation, **"0"** will be returned, and the resource belongs to the default enterprise project. Note: **"0"** is not a valid enterprise project ID and cannot be used in the APIs for creating, updating the load balancer, or querying the details of the load balancer.
billing_info	String	Provides resource billing information. • If the value is left blank, the resource is billed in pay-per-use mode. This parameter is unsupported. Please do not use it.

Parameter	Type	Description
l4_flavor_id	String	Specifies the ID of a flavor at Layer 4. **l4_flavor_id** defines the maximum elastic flavor at Layer 4. Note: • If **l4_flavor_id** is specified, the load balancer is billed by fixed specifications. • If **L4_elastic_max** is specified, the load balancer is billed by how many LCUs you use.
l4_scale_flavor_id	String	Specifies the ID of the reserved flavor at Layer 4. This parameter is unsupported. Please do not use it.
l7_flavor_id	String	Specifies the ID of a flavor at Layer 7. **l7_flavor_id** defines the maximum elastic flavor at Layer 7. Note: • If **l7_flavor_id** is specified, the load balancer is billed by fixed specifications. • If **L7_elastic_max** is specified, the load balancer is billed by how many LCUs you use.
l7_scale_flavor_id	String	Specifies the ID of the reserved flavor at Layer 7. This parameter is unsupported. Please do not use it.
publicips	Array of **PublicIpInfo** objects	Specifies the EIP bound to the load balancer. Only one EIP can be bound to a load balancer. This parameter has the same meaning as **eips**.
global_eips	Array of **GlobalEipInfo** objects	Specifies the global EIP bound to the load balancer. Only the first global EIP specified under **global_eips** will be bound.
elb_virsubnet_ids	Array of strings	Lists the IDs of subnets on the downstream plane.

Parameter	Type	Description
elb_virsubnet_type	String	Specifies the type of the subnet on the downstream plane. Value options: ● **ipv4**: IPv4 subnet ● **dualstack**: subnet that supports IPv4/IPv6 dual stack
ip_target_enable	Boolean	Specifies whether to add backend servers that are not in the load balancer's VPC. If you enable this function, you can add servers in a peer VPC connected through a VPC peering connection, servers in other public clouds, or servers in an on-premises data center at the other end of a Direct Connect or VPN connection, by using their IP addresses. Value options: ● **true**: Enable **IP as a Backend**. ● **false**: Disable **IP as a Backend**. Note: ● The value can only be updated to **true**. ● If you need to connect your server to a shared VPC, ensure the VPC principal has created a VPC peering connections between the two VPCs. ● This function is supported only by dedicated load balancers.

Parameter	Type	Description
frozen_scene	String	Specifies the scenario where the load balancer is frozen. Multiple values are separated using commas (,). Value options: • **POLICE**: The load balancer is frozen due to security reasons. • **ILLEGAL**: The load balancer is frozen due to violation of laws and regulations. • **VERIFY**: Your account has not completed real-name authentication. • **PARTNER**: The load balancer is frozen by the partner. • **ARREAR**: Your account is in arrears.
ipv6_bandwidth	**BandwidthRef** object	Specifies the ID of the bandwidth used by an IPv6 address. Note: This parameter is available only when you create or update a load balancer with a public IPv6 address. If you use a new IPv6 address and specify a shared bandwidth, the IPv6 address will be added to the shared bandwidth.
deletion_protection_enable	Boolean	Specifies whether to enable deletion protection. Value options: • **true**: Enable deletion protection. • **false**: Disable deletion protection. Note: • Disable deletion protection for all your resources before deleting your account. • This parameter is returned only when deletion protection is enabled at the site.

Parameter	Type	Description
autoscaling	**AutoscalingRef** object	Specifies information about elastic scaling. If elastic scaling is enabled, the load balancer specifications can be automatically adjusted based on incoming traffic. Note: • This parameter is only available for users on the whitelist. • If elastic scaling is enabled, **l4_flavor_id** indicates the ID of the maximum elastic flavor at Layer 4. **l7_flavor_id** indicates the ID of the maximum elastic flavor at Layer 7. • This parameter has been deprecated, but is retained for compatibility purposes. Using this parameter is not recommended. If this parameter is specified, the load balancer with minimum specifications will be created and you will be billed for the minimum specifications.
public_border_group	String	Specifies the AZ group to which the load balancer belongs.
charge_mode	String	Specifies the charge mode when creating a load balancer. Value options: • **flavor**: billed by the fixed specification you select. • **lcu**: billed by how many LCUs you have used. • If this parameter is left blank: – If it is a shared load balancer, it is free. – If it is a dedicated load balancer, it will be billed by the fixed specification you select.

Parameter	Type	Description
waf_failure_action	String	Specifies traffic distributing policies when the WAF is faulty. Value options: • **discard**: Traffic will not be distributed. • **forward** (default): Traffic will be distributed to the default backend servers. Note: This parameter takes effect only when WAF is enabled for the load balancer.
protection_status	String	Specifies the protection status. Value options: • **nonProtection** (default): The load balancer is not protected. • **consoleProtection**: **Modification Protection** is enabled on the console.
protection_reason	String	Specifies why the modification protection is enabled. Note: This parameter is valid only when **protection_status** is set to **consoleProtection**. The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).
log_group_id	String	Specifies the ID of the log group that is associated with the load balancer.
log_topic_id	String	Specifies the ID of the log topic that is associated with the load balancer.

Table 5-142 PoolRef

Parameter	Type	Description
id	String	Specifies the ID of the backend server group.

Table 5-143 ListenerRef

Parameter	Type	Description
id	String	Specifies the listener ID.

Table 5-144 Tag

Parameter	Type	Description
key	String	Specifies the tag key.
value	String	Specifies the tag value.

Table 5-145 EipInfo

Parameter	Type	Description
eip_id	String	Specifies the EIP ID.
eip_address	String	Specifies the EIP.
ip_version	Integer	Specifies the IP version. **4** indicates IPv4, and **6** indicates IPv6.

Table 5-146 PublicIpInfo

Parameter	Type	Description
publicip_id	String	Specifies the EIP ID.
publicip_address	String	Specifies the IP address.
ip_version	Integer	Specifies the IP version. The value can be **4** (IPv4) or **6** (IPv6).

Table 5-147 GlobalEipInfo

Parameter	Type	Description
global_eip_id	String	Specifies the ID of the global EIP.
global_eip_address	String	Specifies the global EIP.

Parameter	Type	Description
ip_version	Integer	Specifies the IP version. The value can be **4** and **6**. **4** indicates an IPv4 address, and **6** indicates an IPv6 address.

Table 5-148 BandwidthRef

Parameter	Type	Description
id	String	Specifies the shared bandwidth ID.

Table 5-149 AutoscalingRef

Parameter	Type	Description
enable	Boolean	Specifies whether to enable elastic scaling for the load balancer. Value options: • **true**: Enable elastic scaling. • **false** (default): Disable elastic scaling.
min_l7_flavor_id	String	Specifies the ID of the minimum elastic flavor at Layer 7. Note: • This parameter cannot be left blank if there are HTTP or HTTPS listeners. • This parameter has been deprecated, but is retained for compatibility purposes. Using this parameter is not recommended. If this parameter is specified, the load balancer with minimum specifications will be created and you will be billed for the minimum specifications.

Example Requests

Adding an AZ

```
POST https://{ELB_Endpoint}/v3/060576782980d5762f9ec014dd2f1148/elb/loadbalancers/
9b663cd9-61e4-483d-b91f-92fc337fecec/availability-zone/batch-add

{
```



```
  "availability_zone_list" : [ "az2", "az3" ]
}
```

Example Responses

Status code: 200

Normal response to POST requests.

```
{
  "request_id" : "6c63d0ac-7beb-451d-a3e0-a066beaea316",
  "loadbalancer" : {
    "id" : "9b663cd9-61e4-483d-b91f-92fc337fecec",
    "project_id" : "060576782980d5762f9ec014dd2f1148",
    "name" : "elb-reset",
    "description" : "",
    "vip_port_id" : null,
    "vip_address" : null,
    "admin_state_up" : true,
    "provisioning_status" : "ACTIVE",
    "operating_status" : "ONLINE",
    "listeners" : [ ],
    "pools" : [ ],
    "tags" : [ ],
    "provider" : "vlb",
    "created_at" : "2021-07-26T02:46:31Z",
    "updated_at" : "2021-07-26T02:46:59Z",
    "vpc_id" : "59cb11ef-f185-49ba-92af-0539e8ff9734",
    "enterprise_project_id" : "0",
    "availability_zone_list" : [ "az1", "az2", "az3" ],
    "ipv6_vip_address" : null,
    "ipv6_vip_virsubnet_id" : null,
    "ipv6_vip_port_id" : null,
    "publicips" : [ {
      "publicip_id" : "0c07e04d-e2f9-41ad-b934-f58a65b6734d",
      "publicip_address" : "97.97.2.171",
      "ip_version" : 4
    } ],
    "elb_virsubnet_ids" : [ "7f817f9c-8731-4002-9e47-18cb8d431787" ],
    "elb_virsubnet_type" : "dualstack",
    "ip_target_enable" : false,
    "autoscaling" : {
      "enable" : false,
      "min_l7_flavor_id" : ""
    },
    "frozen_scene" : null,
    "eips" : [ {
      "eip_id" : "0c07e04d-e2f9-41ad-b934-f58a65b6734d",
      "eip_address" : "97.97.2.171",
      "ip_version" : 4
    } ],
    "guaranteed" : true,
    "billing_info" : null,
    "l4_flavor_id" : "636ba721-935a-4ca5-a685-8076ce0e4148",
    "l4_scale_flavor_id" : null,
    "l7_flavor_id" : null,
    "l7_scale_flavor_id" : null,
    "vip_subnet_cidr_id" : null,
    "public_border_group" : "center",
    "protection_status" : "nonProtection",
    "protection_reason" : ""
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Adding an AZ

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;

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

public class BatchAddAvailableZonesSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        BatchAddAvailableZonesRequest request = new BatchAddAvailableZonesRequest();
        request.withLoadbalancerId("{loadbalancer_id}");
        BatchAddAvailableZonesRequestBody body = new BatchAddAvailableZonesRequestBody();
        List<String> listbodyAvailabilityZoneList = new ArrayList<>();
        listbodyAvailabilityZoneList.add("az2");
        listbodyAvailabilityZoneList.add("az3");
        body.withAvailabilityZoneList(listbodyAvailabilityZoneList);
        request.withBody(body);
        try {
            BatchAddAvailableZonesResponse response = client.batchAddAvailableZones(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 an AZ


```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = BatchAddAvailableZonesRequest()
        request.loadbalancer_id = "{loadbalancer_id}"
        listAvailabilityZoneListbody = [
            "az2",
            "az3"
        ]
        request.body = BatchAddAvailableZonesRequestBody(
            availability_zone_list=listAvailabilityZoneListbody
        )
        response = client.batch_add_available_zones(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 an AZ

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.BatchAddAvailableZonesRequest{}
    request.LoadbalancerId = "{loadbalancer_id}"
    var listAvailabilityZoneListbody = []string{
        "az2",
        "az3",
    }
    request.Body = &model.BatchAddAvailableZonesRequestBody{
        AvailabilityZoneList: listAvailabilityZoneListbody,
    }
    response, err := client.BatchAddAvailableZones(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 POST requests.

Error Codes

See **Error Codes**.

5.6.13 Removing a Load Balancer from AZs

Function

This API is used to remove one or more AZs where a load balancer is working.

NOTE

Removing an AZ may disconnect existing connections. Exercise caution when performing this operation.

Constraints

- This API is only available for dedicated load balancers.

- You cannot remove all AZs where a load balancer is working.

Calling Method

For details, see **Calling APIs**.

URI

POST /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}/availability-zone/batch-remove

Table 5-150 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the ID of the project where the load balancer is used.
loadbalancer_id	Yes	String	Specifies the load balancer ID.

Request Parameters

Table 5-151 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	Specifies the token used for IAM authentication.

Table 5-152 Request body parameters

Parameter	Mandatory	Type	Description
availability_zone_list	Yes	Array of strings	Specifies the removed AZs. This parameter cannot be left blank.

Response Parameters

Status code: 200

Table 5-153 Response body parameters

Parameter	Type	Description
loadbalancer	**LoadBalancer** object	Specifies the load balancer.
request_id	String	Specifies the request ID. Note: The value is automatically generated.

Table 5-154 LoadBalancer

Parameter	Type	Description
id	String	Specifies the load balancer ID.
description	String	Provides supplementary information about the load balancer.
provisioning_status	String	Specifies the provisioning status of the load balancer. Value options: • **ACTIVE**: The load balancer is successfully provisioned. • **PENDING_DELETE**: The load balancer is being deleted.
admin_state_up	Boolean	Specifies whether the load balancer is enabled. Value options: • **true**: indicates the load balancer is enabled. • **false**: indicates the load balancer is disabled.
provider	String	Specifies the provider of the load balancer. The value can only be **vlb**.
pools	Array of **PoolRef** objects	Lists the IDs of backend server groups associated with the load balancer.
listeners	Array of **ListenerRef** objects	Lists the IDs of listeners added to the load balancer.

Parameter	Type	Description
operating_status	String	Specifies the operating status of the load balancer. Value options: • **ONLINE**: indicates that the load balancer is running normally. • **FROZEN**: indicates that the load balancer is frozen.
name	String	Specifies the load balancer name.
project_id	String	Specifies the project ID of the load balancer.
vip_subnet_cidr_id	String	Specifies the ID of the frontend IPv4 subnet where the load balancer resides.
vip_address	String	Specifies the private IPv4 address bound to the load balancer.
vip_port_id	String	Specifies the ID of the port bound to the private IPv4 address of the load balancer.
tags	Array of **Tag** objects	Lists the tags added to the load balancer.
created_at	String	Specifies the time when the load balancer was created, in the format of *yyyy-MM-dd''T''HH:mm:ss''Z''*.
updated_at	String	Specifies the time when the load balancer was updated, in the format of *yyyy-MM-dd''T''HH:mm:ss''Z''*.
guaranteed	Boolean	Specifies whether the load balancer is a dedicated load balancer. Value options: • **true** (default): The load balancer is a dedicated load balancer. • **false**: The load balancer is a shared load balancer.
vpc_id	String	Specifies the ID of the VPC where the load balancer resides.
eips	Array of **EipInfo** objects	Specifies the EIP bound to the load balancer. Only one EIP can be bound to a load balancer. This parameter has the same meaning as **publicips**.

Parameter	Type	Description
ipv6_vip_address	String	Specifies the IPv6 address bound to the load balancer.
ipv6_vip_virsubnet_id	String	Specifies the ID of the IPv6 subnet where the load balancer resides.
ipv6_vip_port_id	String	Specifies the ID of the port bound to the IPv6 address of the load balancer.
availability_zone_list	Array of strings	Specifies the list of AZs where the load balancer is created.
enterprise_project_id	String	Specifies the enterprise project ID. If this parameter is not passed during resource creation, **"0"** will be returned, and the resource belongs to the default enterprise project. Note: **"0"** is not a valid enterprise project ID and cannot be used in the APIs for creating, updating the load balancer, or querying the details of the load balancer.
billing_info	String	Provides resource billing information. ● If the value is left blank, the resource is billed in pay-per-use mode. This parameter is unsupported. Please do not use it.
l4_flavor_id	String	Specifies the ID of a flavor at Layer 4. **l4_flavor_id** defines the maximum elastic flavor at Layer 4. Note: ● If **l4_flavor_id** is specified, the load balancer is billed by fixed specifications. ● If **L4_elastic_max** is specified, the load balancer is billed by how many LCUs you use.
l4_scale_flavor_id	String	Specifies the ID of the reserved flavor at Layer 4. This parameter is unsupported. Please do not use it.

Parameter	Type	Description
l7_flavor_id	String	Specifies the ID of a flavor at Layer 7. **l7_flavor_id** defines the maximum elastic flavor at Layer 7. Note: • If **l7_flavor_id** is specified, the load balancer is billed by fixed specifications. • If **L7_elastic_max** is specified, the load balancer is billed by how many LCUs you use.
l7_scale_flavor_id	String	Specifies the ID of the reserved flavor at Layer 7. This parameter is unsupported. Please do not use it.
publicips	Array of **PublicIpInfo** objects	Specifies the EIP bound to the load balancer. Only one EIP can be bound to a load balancer. This parameter has the same meaning as **eips**.
global_eips	Array of **GlobalEipInfo** objects	Specifies the global EIP bound to the load balancer. Only the first global EIP specified under **global_eips** will be bound.
elb_virsubnet_ids	Array of strings	Lists the IDs of subnets on the downstream plane.
elb_virsubnet_type	String	Specifies the type of the subnet on the downstream plane. Value options: • **ipv4**: IPv4 subnet • **dualstack**: subnet that supports IPv4/IPv6 dual stack

Parameter	Type	Description
ip_target_enable	Boolean	Specifies whether to add backend servers that are not in the load balancer's VPC. If you enable this function, you can add servers in a peer VPC connected through a VPC peering connection, servers in other public clouds, or servers in an on-premises data center at the other end of a Direct Connect or VPN connection, by using their IP addresses. Value options: • **true**: Enable **IP as a Backend**. • **false**: Disable **IP as a Backend**. Note: • The value can only be updated to **true**. • If you need to connect your server to a shared VPC, ensure the VPC principal has created a VPC peering connections between the two VPCs. • This function is supported only by dedicated load balancers.
frozen_scene	String	Specifies the scenario where the load balancer is frozen. Multiple values are separated using commas (,). Value options: • **POLICE**: The load balancer is frozen due to security reasons. • **ILLEGAL**: The load balancer is frozen due to violation of laws and regulations. • **VERIFY**: Your account has not completed real-name authentication. • **PARTNER**: The load balancer is frozen by the partner. • **ARREAR**: Your account is in arrears.

Parameter	Type	Description
ipv6_bandwidth	**BandwidthRef** object	Specifies the ID of the bandwidth used by an IPv6 address. Note: This parameter is available only when you create or update a load balancer with a public IPv6 address. If you use a new IPv6 address and specify a shared bandwidth, the IPv6 address will be added to the shared bandwidth.
deletion_protection_enable	Boolean	Specifies whether to enable deletion protection. Value options: • **true**: Enable deletion protection. • **false**: Disable deletion protection. Note: • Disable deletion protection for all your resources before deleting your account. • This parameter is returned only when deletion protection is enabled at the site.
autoscaling	**AutoscalingRef** object	Specifies information about elastic scaling. If elastic scaling is enabled, the load balancer specifications can be automatically adjusted based on incoming traffic. Note: • This parameter is only available for users on the whitelist. • If elastic scaling is enabled, **l4_flavor_id** indicates the ID of the maximum elastic flavor at Layer 4. **l7_flavor_id** indicates the ID of the maximum elastic flavor at Layer 7. • This parameter has been deprecated, but is retained for compatibility purposes. Using this parameter is not recommended. If this parameter is specified, the load balancer with minimum specifications will be created and you will be billed for the minimum specifications.
public_border_group	String	Specifies the AZ group to which the load balancer belongs.

Parameter	Type	Description
charge_mode	String	Specifies the charge mode when creating a load balancer. Value options: • **flavor**: billed by the fixed specification you select. • **lcu**: billed by how many LCUs you have used. • If this parameter is left blank: – If it is a shared load balancer, it is free. – If it is a dedicated load balancer, it will be billed by the fixed specification you select.
waf_failure_action	String	Specifies traffic distributing policies when the WAF is faulty. Value options: • **discard**: Traffic will not be distributed. • **forward** (default): Traffic will be distributed to the default backend servers. Note: This parameter takes effect only when WAF is enabled for the load balancer.
protection_status	String	Specifies the protection status. Value options: • **nonProtection** (default): The load balancer is not protected. • **consoleProtection**: **Modification Protection** is enabled on the console.
protection_reason	String	Specifies why the modification protection is enabled. Note: This parameter is valid only when **protection_status** is set to **consoleProtection**. The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).
log_group_id	String	Specifies the ID of the log group that is associated with the load balancer.
log_topic_id	String	Specifies the ID of the log topic that is associated with the load balancer.

Table 5-155 PoolRef

Parameter	Type	Description
id	String	Specifies the ID of the backend server group.

Table 5-156 ListenerRef

Parameter	Type	Description
id	String	Specifies the listener ID.

Table 5-157 Tag

Parameter	Type	Description
key	String	Specifies the tag key.
value	String	Specifies the tag value.

Table 5-158 EipInfo

Parameter	Type	Description
eip_id	String	Specifies the EIP ID.
eip_address	String	Specifies the EIP.
ip_version	Integer	Specifies the IP version. **4** indicates IPv4, and **6** indicates IPv6.

Table 5-159 PublicIpInfo

Parameter	Type	Description
publicip_id	String	Specifies the EIP ID.
publicip_address	String	Specifies the IP address.
ip_version	Integer	Specifies the IP version. The value can be **4** (IPv4) or **6** (IPv6).

Table 5-160 GlobalEipInfo

Parameter	Type	Description
global_eip_id	String	Specifies the ID of the global EIP.
global_eip_address	String	Specifies the global EIP.
ip_version	Integer	Specifies the IP version. The value can be **4** and **6**. **4** indicates an IPv4 address, and **6** indicates an IPv6 address.

Table 5-161 BandwidthRef

Parameter	Type	Description
id	String	Specifies the shared bandwidth ID.

Table 5-162 AutoscalingRef

Parameter	Type	Description
enable	Boolean	Specifies whether to enable elastic scaling for the load balancer. Value options: • **true**: Enable elastic scaling. • **false** (default): Disable elastic scaling.
min_l7_flavor_id	String	Specifies the ID of the minimum elastic flavor at Layer 7. Note: • This parameter cannot be left blank if there are HTTP or HTTPS listeners. • This parameter has been deprecated, but is retained for compatibility purposes. Using this parameter is not recommended. If this parameter is specified, the load balancer with minimum specifications will be created and you will be billed for the minimum specifications.

Example Requests

Removing an AZ

```
POST https://{ELB_Endpoint}/v3/060576782980d5762f9ec014dd2f1148/elb/loadbalancers/
9b663cd9-61e4-483d-b91f-92fc337fecec/availability-zone/batch-remove

{
  "availability_zone_list" : [ "az2", "az3" ]
}
```

Example Responses

Status code: 200

Normal response to POST requests.


```
{
  "request_id" : "6c63d0ac-7beb-451d-a3e0-a066beaea316",
  "loadbalancer" : {
    "id" : "9b663cd9-61e4-483d-b91f-92fc337fecec",
    "project_id" : "060576782980d5762f9ec014dd2f1148",
    "name" : "elb-reset",
    "description" : "",
    "vip_port_id" : null,
    "vip_address" : null,
    "admin_state_up" : true,
    "provisioning_status" : "ACTIVE",
    "operating_status" : "ONLINE",
    "listeners" : [ ],
    "pools" : [ ],
    "tags" : [ ],
    "provider" : "vlb",
    "created_at" : "2021-07-26T02:46:31Z",
    "updated_at" : "2021-07-26T02:46:59Z",
    "vpc_id" : "59cb11ef-f185-49ba-92af-0539e8ff9734",
    "enterprise_project_id" : "0",
    "availability_zone_list" : [ "az1" ],
    "ipv6_vip_address" : null,
    "ipv6_vip_virsubnet_id" : null,
    "ipv6_vip_port_id" : null,
    "publicips" : [ {
      "publicip_id" : "0c07e04d-e2f9-41ad-b934-f58a65b6734d",
      "publicip_address" : "97.97.2.171",
      "ip_version" : 4
    } ],
    "elb_virsubnet_ids" : [ "7f817f9c-8731-4002-9e47-18cb8d431787" ],
    "elb_virsubnet_type" : "dualstack",
    "ip_target_enable" : false,
    "autoscaling" : {
      "enable" : false,
      "min_l7_flavor_id" : ""
    },
    "frozen_scene" : null,
    "eips" : [ {
      "eip_id" : "0c07e04d-e2f9-41ad-b934-f58a65b6734d",
      "eip_address" : "97.97.2.171",
      "ip_version" : 4
    } ],
    "guaranteed" : true,
    "billing_info" : null,
    "l4_flavor_id" : "636ba721-935a-4ca5-a685-8076ce0e4148",
    "l4_scale_flavor_id" : null,
    "l7_flavor_id" : null,
    "l7_scale_flavor_id" : null,
    "vip_subnet_cidr_id" : null,
    "public_border_group" : "center",
    "protection_status" : "nonProtection",
```



```
    "protection_reason" : ""
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Removing an AZ

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;

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

public class BatchRemoveAvailableZonesSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        BatchRemoveAvailableZonesRequest request = new BatchRemoveAvailableZonesRequest();
        request.withLoadbalancerId("{loadbalancer_id}");
        BatchRemoveAvailableZonesRequestBody body = new BatchRemoveAvailableZonesRequestBody();
        List<String> listbodyAvailabilityZoneList = new ArrayList<>();
        listbodyAvailabilityZoneList.add("az2");
        listbodyAvailabilityZoneList.add("az3");
        body.withAvailabilityZoneList(listbodyAvailabilityZoneList);
        request.withBody(body);
        try {
            BatchRemoveAvailableZonesResponse response = client.batchRemoveAvailableZones(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

Removing an AZ

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = BatchRemoveAvailableZonesRequest()
        request.loadbalancer_id = "{loadbalancer_id}"
        listAvailabilityZoneListbody = [
            "az2",
            "az3"
        ]
        request.body = BatchRemoveAvailableZonesRequestBody(
            availability_zone_list=listAvailabilityZoneListbody
        )
        response = client.batch_remove_available_zones(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

Removing an AZ

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.BatchRemoveAvailableZonesRequest{}
    request.LoadbalancerId = "{loadbalancer_id}"
    var listAvailabilityZoneListbody = []string{
        "az2",
        "az3",
    }
    request.Body = &model.BatchRemoveAvailableZonesRequestBody{
        AvailabilityZoneList: listAvailabilityZoneListbody,
    }
    response, err := client.BatchRemoveAvailableZones(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 POST requests.

Error Codes

See **Error Codes**.

5.7 Certificate

5.7.1 Creating a Certificate

Function

This API is used to create an SSL certificate for HTTPS listeners.

Calling Method

For details, see **Calling APIs**.

URI

POST /v3/{project_id}/elb/certificates

Table 5-163 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Request Parameters

Table 5-164 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Table 5-165 Request body parameters

Parameter	Mandatory	Type	Description
certificate	Yes	**CreateCertificateOption** object	Specifies the certificate.

Table 5-166 CreateCertificateOption

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Specifies the administrative status of the certificate. This parameter is unsupported. Please do not use it.

Parameter	Mandatory	Type	Description
certificate	No	String	Specifies the body of the certificate required by HTTPS listeners. The value must be PEM encoded. Maximum 65,536-character length is allowed, supports certificate chains with a maximum of 11 layers (including certificates and certificate chains).
description	No	String	Provides supplementary information about the certificate.
domain	No	String	Specifies the domain names used by the server certificate. This parameter will take effect only when **type** is set to **server**. Note the following when specifying a domain name: ● The value can contain 0 to 10,000 characters and consists of multiple common domain names or wildcard domain names separated by commas. A maximum of 100 domain names are allowed. ● A common domain name consists of several labels separated by periods (.). Each label can contain a maximum of 63 characters, including letters, digits, and hyphens (-), and must start and end with a letter or digit. Example: www.test.com ● A wildcard domain name is a domain name that starts with *. Example: *.test.com
name	No	String	Specifies the certificate name.

Parameter	Mandatory	Type	Description
private_key	No	String	Specifies the private key of the certificate used by HTTPS listeners. The value can contain up to 8,192 PEM encoded characters. • This parameter is valid and mandatory only when **type** is set to **server**. • This parameter will be ignored even if **type** is set to **client**. The value must be PEM encoded and will not take effect.
project_id	No	String	• This parameter is valid and mandatory only when **type** is set to **server**.
type	No	String	Specifies the certificate type. The value can be **server** or **client**. **server** indicates server certificates, and **client** indicates CA certificates. The default value is **server**.
enterprise_project_id	No	String	Specifies the ID of the enterprise project that the certificate belongs to.
enc_certificate	No	String	Specifies the body of the SM encryption certificate required by HTTPS listeners. The value must be PEM encoded. Maximum 65,536-character length is allowed, supports certificate chains with a maximum of 11 layers (including certificates and certificate chains). This parameter is mandatory only when **type** is set to **server_sm**.

Parameter	Mandatory	Type	Description
enc_private_key	No	String	Specifies the private key of the SM encryption certificate required by HTTPS listeners. The value must be PEM encoded. Maximum 8,192-character length is allowed. This parameter is mandatory only when **type** is set to **server_sm**.
scm_certificate_id	No	String	Specifies the SM certificate ID.

Response Parameters

Status code: 201

Table 5-167 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
certificate	**CertificateInfo** object	Specifies the certificate.

Table 5-168 CertificateInfo

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the certificate. This parameter is unsupported. Please do not use it.
certificate	String	Specifies the certificate content. The value must be PEM encoded.
description	String	Provides supplementary information about the certificate.

Parameter	Type	Description
domain	String	Specifies the domain names used by the server certificate. This parameter will take effect only when **type** is set to **server**. Note the following when specifying a domain name: ● The value can contain 0 to 10,000 characters and consists of multiple common domain names or wildcard domain names separated by commas. A maximum of 100 domain names are allowed. ● A common domain name consists of several labels separated by periods (.). Each label can contain a maximum of 63 characters, including letters, digits, and hyphens (-), and must start and end with a letter or digit. Example: www.test.com ● A wildcard domain name is a domain name that starts with *. Example: *.test.com
id	String	Specifies the certificate ID.
name	String	Specifies the certificate name.
private_key	String	Specifies the private key of the certificate used by HTTPS listeners. The value must be PEM encoded characters. ● This parameter will be ignored even if **type** is set to **client**. The certificate can still be created and used normally. ● This parameter is valid and mandatory only when **type** is set to **server**.
type	String	Specifies the certificate type. The value can be **server** or **client**. **server** indicates server certificates, and **client** indicates CA certificates. The default value is **server**.
created_at	String	Specifies the time when the certificate was created.

Parameter	Type	Description
updated_at	String	Specifies the time when the certificate was updated.
expire_time	String	Specifies the time when the certificate expires.
project_id	String	Specifies the project ID of the certificate.
enc_certificate	String	Specifies the body of the SM encryption certificate required by HTTPS listeners. The value must be PEM encoded. Note: This parameter is returned only when the SM encryption certificate feature is enabled at the site.
enc_private_key	String	Specifies the private key of the SM encryption certificate required by HTTPS listeners. The value must be PEM encoded. Note: This parameter is returned only when the SM encryption certificate feature is enabled at the site.
scm_certificate_id	String	Specifies the SSL certificate ID.
common_name	String	Specifies the primary domain name of the certificate.
fingerprint	String	Specifies the fingerprint of the certificate.
subject_alternative_names	Array of strings	Specifies all the domain names of the certificate.

Example Requests

Creating a server certificate and specifying the private key used by the HTTPS listener

```
POST https://{ELB_Endpoint}/v3/{project_id}/elb/certificates

{
  "certificate" : {
    "name" : "My Certificate",
    "type" : "server",
    "private_key" : "-----BEGIN PRIVATE KEY-----
\nMIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDQVAbOLe5xNf4M
\n253Wn9vhdUzojetjv4J+B7kYwsMhRcgdcJ8KCnX1nfzTvI2ksXlTQ2o9BkpStnPe\ntB4s32ZiJRMlk
+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM
\nMD30gLh6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8Icq39buNpIgDOWzEP5AzqXt
\nCOFYn6RTH5SRug4hKNN7sT1eYMslHu7wtEBDKVgrLjOCe/W2f8rLT1zEsoAW2Chl\nZAPYUBkl/
0XuTWRg3CohPPcI+UtlRSfvLDeeQ460swjbwgS/RbJh3sIwlCRLU08k\nEo04Z9H/
```


AgMBAAECggEAEIeaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/Hl
\nfvCArftGgMaYWPSNCJRMXB7tPwpQu19esjz4Z/cR2Je4fTLPrffGUsHFgZjv5OQB
\nZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr\nciu9YkInNEHu6uRJ5g/
eGGX3KQynTvVIhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M\nEGpfYI6AdHIwFZcT/
RNAxhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7Ale\nkrguPtfV1vWklg
+bUFhgGaiAEYTpAUN9t2DVIiijgQKBgQDnYMMsaF0r557CM1CT
\nXUqgCZo8MKeV2jf2drlxRRwRl33SksQbzAQ/qrLdT7GP3sCGqvkxWY2FPdFYf8kx
\nGcCeZPcIeZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/fbwjpjP7dt
\nJ7n8EzkRUNE6aIMHOFEeych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr
\niWgTWHXPZxUQaYhpjXo6+lMI6DpExiDgBAkMzJGIvS7yQiYWU+wthAr9urbWYdGZ
\nlS6VjoTkF6r7VZoILXX0fbuXh6lm8K8IQRfBpJff56p9phMwaBpDNDrfpHB5utBU\nxs40yIdp6wKBgQC69Cp/
xUwTX7GdxQzEJctYiKnBHKcspAg38zJf3bGSXU/jR4eB\n1lVQhELGI9CbKSdzKM71GyEImix/
T7FnJSHIWlho1qVo6AQyduNWnAQD15pr8KAd\nXGXAZZ1FQcb3KYa
+2fflERmazdOTwjYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak\n/735uP20KKqhNehZpC2dJei7OiIgRhCS/
dKASUXHSW4fptBnUxACYocdDxtY4Vha\nfI7FPMdvGl8ioYbvlHFh
+X0Xs9r1S8yeWnHoXMb6eXWmYKMJrAoveLa+2cFm1Agf
\n7nLhA4R4lqm9IpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAJkD4wHW54Pwd4Ctfk9o
\njHjWB7pQlUYpTZO9dm+4fpCMn9Okf43AE2yAOaAP94GdzdDJkxfciXKcsYr9IIuk
\nfaoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BUlGKMWXzuEd\n3fy
+1rCUwzOp9LSjtJYf4ege\n-----END PRIVATE KEY-----",
"certificate" : "-----BEGIN CERTIFICATE-----
\nMIIC4TCCAcmgAwIBAgICEREwDQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXlD
\nb21wYW55IENBMB4XDTE4MDcwMjEzMjU0N1oXDTQ1MTExNzEzMjU0N1owFDESMBAG
\nA1UEAwwJbG9jYWxob3N0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA\n0FQGzi3ucTX
+DNud1p/
b4XVM6I3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5\nU0NqPQZKUrZz3rQeLN9mYiUTJZPutYlFDDbB8Ctl
gV+eyU9yYJslWx/Bm5kWNPh9\n7B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/
W7jaS\nIAzlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylYKy4zgnv1tn/K
\ny09cxLKAFtgoZWQD2FAZJf9F7k1kYNwqITz3CPlLZUUn7yw3nkOOtLMI28IEv0Wy
\nYd7CMJQkS1NPJBKNOGfR/wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29t\nhwQKuUvJhwR/
AAABMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCSqGSIb3DQEBCwUA
\nA4IBAQA8lMQJxaTey7EjXtRLSVlEAMftAQPG6jijNQuvIBQYUDauDT4W2XUZ5wAn
\njiOyQ83va672K1G9s8n6xlH+xwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDa
\nezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPRLYlzp1HMnI6hkjPk4PCZ
\nwKnha0dlScati9CCt3UzXSNJOSLalKdHErH08Iqd+1BchScxCfk0xNITn1HZZGmI\n
+vbmunok3A2lucI14rnsrcbkGYqxGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZ\niYsGDVN+9QBd0eYUHce
+77s96i3I\n-----END CERTIFICATE-----"
}
}

Example Responses

Status code: 201

Normal response to POST requests.

{
"certificate" : {
"private_key" : "-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDQVAbOLe5xNf4M253Wn9vhdUzojetjv4J
+B7kYwsMhRcgdcJ8KCnX1nfzTvI2ksXlTQ2o9BkpStnPetB4s32ZiJRMlk
+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rMMD30gLh6QoP3cq7PGWcuZKV7hjd1tjCT
QukwMvqV8Icq39buNpIgDOWzEP5AzqXtCOFYn6RTH5SRug4hKNN7sT1eYMslHu7wtEBDKVgrLjOCe/
W2f8rLT1zEsoAW2ChlZAPYUBkl/0XuTWRg3CohPPcI+UtlRSfvLDeeQ460swjbwgS/RbJh3sIwlCRLU08kEo04Z9H/
AgMBAAECggEAEIeaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/
HlfvCArftGgMaYWPSNCJRMXB7tPwpQu19esjz4Z/
cR2Je4fTLPrffGUsHFgZjv5OQBZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNK
Krciu9YkInNEHu6uRJ5g/eGGX3KQynTvVIhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9MEGpfYI6AdHIwFZcT/
RNAxhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7AlekrguPtfV1vWklg
+bUFhgGaiAEYTpAUN9t2DVIiijgQKBgQDnYMMsaF0r557CM1CTXUqgCZo8MKeV2jf2drlxRRwRl33SksQbzAQ/
qrLdT7GP3sCGqvkxWY2FPdFYf8kxGcCeZPcIeZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/
fbwjpjP7dtJ7n8EzkRUNE6aIMHOFEeych/
PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLriWgTWHXPZxUQaYhpjXo6+lMI6DpExiDgBAkMzJGIvS7y
QiYWU
+wthAr9urbWYdGZlS6VjoTkF6r7VZoILXX0fbuXh6lm8K8IQRfBpJff56p9phMwaBpDNDrfpHB5utBUxs40yIdp6w
KBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zJf3bGSXU/jR4eB1lVQhELGI9CbKSdzKM71GyEImix/
T7FnJSHIWlho1qVo6AQyduNWnAQD15pr8KAdXGXAZZ1FQcb3KYa
+2fflERmazdOTwjYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak/735uP20KKqhNehZpC2dJei7OiIgRhCS/
dKASUXHSW4fptBnUxACYocdDxtY4VhafI7FPMdvGl8ioYbvlHFh+X0Xs9r1S8yeWnHoXMb6eXWmYKMJrAoveLa

+2cFm1Agf7nLhA4R4lqm9IpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAJkD4wHW54Pwd4Ctfk9ojHjWB7pQlUYpT
ZO9dm
+4fpCMn9Okf43AE2yAOaAP94GdzdDJkxfciXKcsYr9IIukfaoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO3
8a5gZaOm/BUlGKMWXzuEd3fy+1rCUwzOp9LSjtJYf4ege-----END PRIVATE KEY-----",
    "description" : "",
    "domain" : null,
    "created_at" : "2019-03-31T22:23:51Z",
    "expire_time" : "2045-11-17T13:25:47Z",
    "id" : "233a325e5e3e4ce8beeb320aa714cc12",
    "name" : "My Certificate",
    "certificate" : "-----BEGIN CERTIFICATE-----
MIIC4TCCAcmgAwIBAgICEREwDQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXlDb21wYW55IENBMB4X
DTE4MDcwMjEzMjU0N1oXDTQ1MTExNzEzMjU0N1owFDESMBAGA1UEAwwJbG9jYWxob3N0MIIBIjANBgkqh
kiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0FQGzi3ucTX+DNud1p/
b4XVM6I3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5U0NqPQZKUrZz3rQeLN9mYiUTJZPutYlFDDbB8CtlgV
+eyU9yYJslWx/Bm5kWNPh97B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/
W7jaSIAzlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylYKy4zgnv1tn/
Ky09cxLKAFtgoZWQD2FAZJf9F7k1kYNwqITz3CPlLZUUn7yw3nkOOtLMI28IEv0WyYd7CMJQkS1NPJBKNOGfR/
wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29thwQKuUvJhwR/
AAABMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCSqGSIb3DQEBCwUAA4IBAQA8lMQJxaTey7EjXtRLSVl
EAMftAQPG6jijNQuvIBQYUDauDT4W2XUZ5wAnjiOyQ83va672K1G9s8n6xlH
+xwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDaezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPR
LYlzp1HMnI6hkjPk4PCZwKnha0dlScati9CCt3UzXSNJOSLalKdHErH08Iqd+1BchScxCfk0xNITn1HZZGmI
+vbmunok3A2lucI14rnsrcbkGYqxGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZiYsGDVN+9QBd0eYUHce
+77s96i3I-----END CERTIFICATE-----",
    "admin_state_up" : true,
    "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
    "updated_at" : "2019-03-31T23:26:49Z",
    "type" : "server",
    "common_name" : "www.example.com",
    "fingerprint" : "869df7fcb441c2ef3fb9329437815972eeb1ef0e",
    "subject_alternative_names" : ["www.example.com"]
  },
  "request_id" : "98414965-856c-4be3-8a33-3e08432a222e"
}

SDK Sample Code

The SDK sample code is as follows.

Java

Creating a server certificate and specifying the private key used by the HTTPS listener

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class CreateCertificateSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateCertificateRequest request = new CreateCertificateRequest();
        CreateCertificateRequestBody body = new CreateCertificateRequestBody();
        CreateCertificateOption certificatebody = new CreateCertificateOption();
        certificatebody.withCertificate("-----BEGIN CERTIFICATE-----
MIIC4TCCAcmgAwIBAgICEREwDQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXlD
b21wYW55IENBMB4XDTE4MDcwMjEzMjU0N1oXDTQ1MTExNzEzMjU0N1owFDESMBAG
A1UEAwwJbG9jYWxob3N0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
0FQGzi3ucTX+DNud1p/b4XVM6I3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5
U0NqPQZKUrZz3rQeLN9mYiUTJZPutYlFDDbB8CtlgV+eyU9yYJslWx/Bm5kWNPh9
7B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/W7jaS
IAzlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylYKy4zgnv1tn/K
y09cxLKAFtgoZWQD2FAZJf9F7k1kYNwqITz3CPlLZUUn7yw3nkOOtLMI28IEv0Wy
Yd7CMJQkS1NPJBKNOGfR/wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29t
hwQKuUvJhwR/AAABMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCSqGSIb3DQEBCwUA
A4IBAQA8lMQJxaTey7EjXtRLSVlEAMftAQPG6jijNQuvIBQYUDauDT4W2XUZ5wAn
jiOyQ83va672K1G9s8n6xlH+xwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDa
ezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPRLYlzp1HMnI6hkjPk4PCZ
wKnha0dlScati9CCt3UzXSNJOSLalKdHErH08Iqd+1BchScxCfk0xNITn1HZZGmI
+vbmunok3A2lucI14rnsrcbkGYqxGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZ
iYsGDVN+9QBd0eYUHce+77s96i3I
-----END CERTIFICATE-----")
                .withName("My Certificate")
                .withPrivateKey("-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDQVAbOLe5xNf4M
253Wn9vhdUzojetjv4J+B7kYwsMhRcgdcJ8KCnX1nfzTvI2ksXlTQ2o9BkpStnPe
tB4s32ZiJRMlk+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM
MD30gLh6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8Icq39buNpIgDOWzEP5AzqXt
COFYn6RTH5SRug4hKNN7sT1eYMslHu7wtEBDKVgrLjOCe/W2f8rLT1zEsoAW2Chl
ZAPYUBkl/0XuTWRg3CohPPcI+UtlRSfvLDeeQ460swjbwgS/RbJh3slwlCRLU08k
Eo04Z9H/AgMBAAECggEAEIeaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/Hl
fvCArftGgMaYWPSNCJRMXB7tPwpQu19esjz4Z/cR2Je4fTLPrffGUsHFgZjv5OQB
ZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr
ciu9YkInNEHu6uRJ5g/eGGX3KQynTvVIhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M
EGpfYI6AdHIwFZcT/RNAxhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7Ale
krguPtfV1vWklg+bUFhgGaiAEYTpAUN9t2DVIiijgQKBgQDnYMMsaF0r557CM1CT
XUqgCZo8MKeV2jf2drlxRRwRl33SksQbzAQ/qrLdT7GP3sCGqvkxWY2FPdFYf8kx
GcCeZPcIeZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/fbwjpjP7dt
J7n8EzkRUNE6aIMHOFEeych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr
iWgTWHXPZxUQaYhpjXo6+lMI6DpExiDgBAkMzJGIvS7yQiYWU+wthAr9urbWYdGZ
lS6VjoTkF6r7VZoILXX0fbuXh6lm8K8IQRfBpJff56p9phMwaBpDNDrfpHB5utBU
xs40yIdp6wKBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zJf3bGSXU/jR4eB
1lVQhELGI9CbKSdzKM71GyEImix/T7FnJSHIWlho1qVo6AQyduNWnAQD15pr8KAd
XGXAZZ1FQcb3KYa+2fflERmazdOTwjYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak
/735uP20KKqhNehZpC2dJei7OiIgRhCS/dKASUXHSW4fptBnUxACYocdDxtY4Vha
fI7FPMdvGl8ioYbvlHFh+X0Xs9r1S8yeWnHoXMb6eXWmYKMJrAoveLa+2cFm1Agf
7nLhA4R4lqm9IpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAJkD4wHW54Pwd4Ctfk9o
jHjWB7pQlUYpTZO9dm+4fpCMn9Okf43AE2yAOaAP94GdzdDJkxfciXKcsYr9IIuk
faoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BUlGKMWXzuEd
3fy+1rCUwzOp9LSjtJYf4ege
-----END PRIVATE KEY-----")
                .withType(CreateCertificateOption.TypeEnum.fromValue("server"));
        body.withCertificate(certificatebody);
        request.withBody(body);
        try {
            CreateCertificateResponse response = client.createCertificate(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

Creating a server certificate and specifying the private key used by the HTTPS listener

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateCertificateRequest()
        certificatebody = CreateCertificateOption(
            certificate="-----BEGIN CERTIFICATE-----
        MIIC4TCCAcmgAwIBAgICEREwDQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXlD
        b21wYW55IENBMB4XDTE4MDcwMjEzMjU0N1oXDTQ1MTExNzEzMjU0N1owFDESMBAG
        A1UEAwwJbG9jYWxob3N0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
        0FQGzi3ucTX+DNud1p/b4XVM6I3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5
        U0NqPQZKUrZz3rQeLN9mYiUTJZPutYlFDDbB8CtlgV+eyU9yYJslWx/Bm5kWNPh9
        7B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/W7jaS
        IAzlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylYKy4zgnv1tn/K
        y09cxLKAFtgoZWQD2FAZJf9F7k1kYNwqITz3CPlLZUUn7yw3nkOOtLMI28IEv0Wy
        Yd7CMJQkS1NPJBKNOGfR/wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29t
        hwQKuUvJhwR/AAABMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCSqGSIb3DQEBCwUA
        A4IBAQA8lMQJxaTey7EjXtRLSVlEAMftAQPG6jijNQuvIBQYUDauDT4W2XUZ5wAn
        jiOyQ83va672K1G9s8n6xlH+xwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDa
        ezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPRLYlzp1HMnI6hkjPk4PCZ
        wKnha0dlScati9CCt3UzXSNJOSLalKdHErH08Iqd+1BchScxCfk0xNITn1HZZGmI
        +vbmunok3A2lucI14rnsrcbkGYqxGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZ
        iYsGDVN+9QBd0eYUHce+77s96i3I
        -----END CERTIFICATE-----",
            name="My Certificate",
            private_key="-----BEGIN PRIVATE KEY-----
        MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDQVAbOLe5xNf4M
        253Wn9vhdUzojetjv4J+B7kYwsMhRcgdcJ8KCnX1nfzTvI2ksXlTQ2o9BkpStnPe
        tB4s32ZiJRMlk+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM
        MD30gLh6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8Icq39buNpIgDOWzEP5AzqXt
```

```
        COFYn6RTH5SRug4hKNN7sT1eYMslHu7wtEBDKVgrLjOCe/W2f8rLT1zEsoAW2Chl
        ZAPYUBkl/0XuTWRg3CohPPcI+UtlRSfvLDeeQ460swjbwgS/RbJh3sIwlCRLU08k
        Eo04Z9H/AgMBAAECggEAEIeaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/Hl
        fvCArftGgMaYWPSNCJRMXB7tPwpQu19esjz4Z/cR2Je4fTLPrffGUsHFgZjv5OQB
        ZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr
        ciu9YkInNEHu6uRJ5g/eGGX3KQynTvVIhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M
        EGpfYI6AdHIwFZcT/RNAxhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7Ale
        krguPtfV1vWklg+bUFhgGaiAEYTpAUN9t2DVIiijgQKBgQDnYMMsaF0r557CM1CT
        XUqgCZo8MKeV2jf2drlxRRwRl33SksQbzAQ/qrLdT7GP3sCGqvkxWY2FPdFYf8kx
        GcCeZPcIeZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/fbwjpjP7dt
        J7n8EzkRUNE6aIMHOFEeych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr
        iWgTWHXPZxUQaYhpjXo6+lMI6DpExiDgBAkMzJGIvS7yQiYWU+wthAr9urbWYdGZ
        lS6VjoTkF6r7VZoILXX0fbuXh6lm8K8IQRfBpJff56p9phMwaBpDNDrfpHB5utBU
        xs40yIdp6wKBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zJf3bGSXU/jR4eB
        1lVQhELGI9CbKSdzKM71GyEImix/T7FnJSHIWlho1qVo6AQyduNWnAQD15pr8KAd
        XGXAZZ1FQcb3KYa+2fflERmazdOTwjYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak
        /735uP20KKqhNehZpC2dJei7OiIgRhCS/dKASUXHSW4fptBnUxACYocdDxtY4Vha
        fI7FPMdvGl8ioYbvlHFh+X0Xs9r1S8yeWnHoXMb6eXWmYKMJrAoveLa+2cFm1Agf
        7nLhA4R4lqm9IpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAJkD4wHW54Pwd4Ctfk9o
        jHjWB7pQlUYpTZO9dm+4fpCMn9Okf43AE2yAOaAP94GdzdDJkxfciXKcsYr9IIuk
        faoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BUlGKMWXzuEd
        3fy+1rCUwzOp9LSjtJYf4ege
        -----END PRIVATE KEY-----",
            type="server"
        )
        request.body = CreateCertificateRequestBody(
            certificate=certificatebody
        )
        response = client.create_certificate(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

Creating a server certificate and specifying the private key used by the HTTPS listener

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
```



```
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

    request := &model.CreateCertificateRequest{}
    certificateCertificate:= "-----BEGIN CERTIFICATE-----
MIIC4TCCAcmgAwIBAgICEREwDQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXlD
b21wYW55IENBMB4XDTE4MDcwMjEzMjU0N1oXDTQ1MTExNzEzMjU0N1owFDESMBAG
A1UEAwwJbG9jYWxob3N0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
0FQGzi3ucTX+DNud1p/b4XVM6I3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5
U0NqPQZKUrZz3rQeLN9mYiUTJZPutYlFDDbB8CtlgV+eyU9yYJslWx/Bm5kWNPh9
7B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/W7jaS
IAzlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylYKy4zgnv1tn/K
y09cxLKAFtgoZWQD2FAZJf9F7k1kYNwqITz3CPlLZUUn7yw3nkOOtLMI28IEv0Wy
Yd7CMJQkS1NPJBKNOGfR/wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29t
hwQKuUvJhwR/AAABMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCSqGSIb3DQEBCwUA
A4IBAQA8lMQJxaTey7EjXtRLSVlEAMftAQPG6jijNQuvIBQYUDauDT4W2XUZ5wAn
jiOyQ83va672K1G9s8n6xlH+xwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDa
ezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPRLYlzp1HMnI6hkjPk4PCZ
wKnha0dlScati9CCt3UzXSNJOSLalKdHErH08Iqd+1BchScxCfk0xNITn1HZZGmI
+vbmunok3A2lucI14rnsrcbkGYqxGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZ
iYsGDVN+9QBd0eYUHce+77s96i3I
-----END CERTIFICATE-----"
    nameCertificate:= "My Certificate"
    privateKeyCertificate:= "-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDQVAbOLe5xNf4M
253Wn9vhdUzojetjv4J+B7kYwsMhRcgdcJ8KCnX1nfzTvI2ksXlTQ2o9BkpStnPe
tB4s32ZiJRMlk+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM
MD30gLh6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8Icq39buNpIgDOWzEP5AzqXt
COFYn6RTH5SRug4hKNN7sT1eYMslHu7wtEBDKVgrLjOCe/W2f8rLT1zEsoAW2Chl
ZAPYUBkl/0XuTWRg3CohPPcI+UtlRSfvLDeeQ460swjbwgS/RbJh3sIwlCRLU08k
Eo04Z9H/AgMBAAECggEAEIeaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/Hl
fvCArftGgMaYWPSNCJRMXB7tPwpQu19esjz4Z/cR2Je4fTLPrffGUsHFgZjv5OQB
ZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr
ciu9YkInNEHu6uRJ5g/eGGX3KQynTvVIhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M
EGpfYI6AdHIwFZcT/RNAxhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7Ale
krguPtfV1vWklg+bUFhgGaiAEYTpAUN9t2DVIiijgQKBgQDnYMMsaF0r557CM1CT
XUqgCZo8MKeV2jf2drlxRRwRl33SksQbzAQ/qrLdT7GP3sCGqvkxWY2FPdFYf8kx
GcCeZPcIeZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/fbwjpjP7dt
J7n8EzkRUNE6aIMHOFEeych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr
iWgTWHXPZxUQaYhpjXo6+lMI6DpExiDgBAkMzJGIvS7yQiYWU+wthAr9urbWYdGZ
lS6VjoTkF6r7VZoILXX0fbuXh6lm8K8IQRfBpJff56p9phMwaBpDNDrfpHB5utBU
xs40yIdp6wKBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zJf3bGSXU/jR4eB
1lVQhELGI9CbKSdzKM71GyEImix/T7FnJSHIWlho1qVo6AQyduNWnAQD15pr8KAd
XGXAZZ1FQcb3KYa+2fflERmazdOTwjYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak
/735uP20KKqhNehZpC2dJei7OiIgRhCS/dKASUXHSW4fptBnUxACYocdDxtY4Vha
fI7FPMdvGl8ioYbvlHFh+X0Xs9r1S8yeWnHoXMb6eXWmYKMJrAoveLa+2cFm1Agf
7nLhA4R4lqm9IpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAJkD4wHW54Pwd4Ctfk9o
jHjWB7pQlUYpTZO9dm+4fpCMn9Okf43AE2yAOaAP94GdzdDJkxfciXKcsYr9IIuk
faoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BUlGKMWXzuEd
3fy+1rCUwzOp9LSjtJYf4ege
-----END PRIVATE KEY-----"
    typeCertificate:= model.GetCreateCertificateOptionTypeEnum().SERVER
    certificatebody := &model.CreateCertificateOption{
        Certificate: &certificateCertificate,
        Name: &nameCertificate,
        PrivateKey: &privateKeyCertificate,
        Type: &typeCertificate,
    }
    request.Body = &model.CreateCertificateRequestBody{
        Certificate: certificatebody,
    }
    response, err := client.CreateCertificate(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 POST requests.

Error Codes

See **Error Codes**.

5.7.2 Querying Certificates

Function

This API is used to query all SSL certificates.

Constraints

This API has the following constraints:

- Parameters **marker**, **limit**, and **page_reverse** are used for pagination query.
- Parameters **marker** and **page_reverse** take effect only when they are used together with parameter **limit**.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/certificates

Table 5-169 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Table 5-170 Query Parameters

Parameter	Mandatory	Type	Description
marker	No	String	Specifies the ID of the last record on the previous page. Note: • This parameter must be used together with **limit**. • If this parameter is not specified, the first page will be queried. • This parameter cannot be left blank or set to an invalid ID.
limit	No	Integer	Specifies the number of records on each page. Value range: 0–2000 Default value: 2000
page_reverse	No	Boolean	Specifies whether to use reverse query. Value options: • **true**: Query the previous page. • **false** (default): Query the next page. Note: • This parameter must be used together with **limit**. • If **page_reverse** is set to **true** and you want to query the previous page, set the value of **marker** to the value of **previous_marker**.
id	No	Array of strings	Specifies a certificate ID. Multiple IDs can be queried in the format of *id=xxx&id=xxx*.
name	No	Array of strings	Specifies the certificate name. Multiple names can be queried in the format of *name=xxx&name=xxx*.

Parameter	Mandatory	Type	Description
description	No	Array of strings	Provides supplementary information about the certificate. Multiple descriptions can be queried in the format of *description=xxx&description=xxx*.
admin_state_up	No	Boolean	Specifies the administrative status of the certificate. This parameter is unsupported. Please do not use it.
domain	No	Array of strings	Specifies the domain names used by the server certificate. This parameter is available only when **type** is set to **server**. Multiple domain names can be queried in the format of *domain=xxx&domain=xxx*.
type	No	Array of strings	Specifies the certificate type. The value can be **server** or **client**. **server** indicates server certificates, and **client** indicates CA certificates. Multiple types can be queried in the format of *type=xxx&type=xxx*.
scm_certificate_id	No	Array of strings	Specifies the SSL certificate ID. Multiple IDs can be queried in the format of *scm_certificate_id=xxx&scm_certificate_id=xxx*.
common_name	No	Array of strings	Specifies the primary domain name of the certificate. Multiple values can be queried in the format of *common_name=xxx&common_name=xxx*.

Parameter	Mandatory	Type	Description
fingerprint	No	Array of strings	Specifies the fingerprint of the certificate. Multiple values can be queried in the format of *fingerprint=xxx&fingerprint=xxx*.

Request Parameters

Table 5-171 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-172 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
page_info	**PageInfo** object	Shows pagination information about certificates.
certificates	Array of **CertificateInfo** objects	Lists the certificates.

Table 5-173 PageInfo

Parameter	Type	Description
previous_marker	String	Specifies the ID of the first record in the pagination query result. When **page_reverse** is set to **true**, this parameter is used together to query resources on the previous page.

Parameter	Type	Description
next_marker	String	Specifies the ID of the last record in the pagination query result.
current_count	Integer	Specifies the number of records.

Table 5-174 CertificateInfo

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the certificate. This parameter is unsupported. Please do not use it.
certificate	String	Specifies the certificate content. The value must be PEM encoded.
description	String	Provides supplementary information about the certificate.
domain	String	Specifies the domain names used by the server certificate. This parameter will take effect only when **type** is set to **server**. Note the following when specifying a domain name: ● The value can contain 0 to 10,000 characters and consists of multiple common domain names or wildcard domain names separated by commas. A maximum of 100 domain names are allowed. ● A common domain name consists of several labels separated by periods (.). Each label can contain a maximum of 63 characters, including letters, digits, and hyphens (-), and must start and end with a letter or digit. Example: www.test.com ● A wildcard domain name is a domain name that starts with *. Example: *.test.com
id	String	Specifies the certificate ID.
name	String	Specifies the certificate name.

Parameter	Type	Description
private_key	String	Specifies the private key of the certificate used by HTTPS listeners. The value must be PEM encoded characters. • This parameter will be ignored even if **type** is set to **client**. The certificate can still be created and used normally. • This parameter is valid and mandatory only when **type** is set to **server**.
type	String	Specifies the certificate type. The value can be **server** or **client**. **server** indicates server certificates, and **client** indicates CA certificates. The default value is **server**.
created_at	String	Specifies the time when the certificate was created.
updated_at	String	Specifies the time when the certificate was updated.
expire_time	String	Specifies the time when the certificate expires.
project_id	String	Specifies the project ID of the certificate.
enc_certificate	String	Specifies the body of the SM encryption certificate required by HTTPS listeners. The value must be PEM encoded. Note: This parameter is returned only when the SM encryption certificate feature is enabled at the site.
enc_private_key	String	Specifies the private key of the SM encryption certificate required by HTTPS listeners. The value must be PEM encoded. Note: This parameter is returned only when the SM encryption certificate feature is enabled at the site.
scm_certificate_id	String	Specifies the SSL certificate ID.
common_name	String	Specifies the primary domain name of the certificate.

Parameter	Type	Description
fingerprint	String	Specifies the fingerprint of the certificate.
subject_alternative_names	Array of strings	Specifies all the domain names of the certificate.

Example Requests

Querying certificates

```
GET https://{ELB_Endpoint}/v3/{project_id}/elb/certificates
```

Example Responses

Status code: 200

Successful request.


```
{
  "certificates" : [ {
    "id" : "5494a835d88f40ff940554992f2f04d4",
    "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
    "name" : "https_certificatekkkk",
    "type" : "server",
    "domain" : null,
    "description" : "description for certificatehhhh",
    "private_key" : "-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDQVAbOLe5xNf4M253Wn9vhdUzojetjv4J
+B7kYwsMhRcgdcJ8KCnX1nfzTvI2ksXlTQ2o9BkpStnPetB4s32ZiJRMlk
+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rMMD30gLh6QoP3cq7PGWcuZKV7hjd1tjCT
QukwMvqV8Icq39buNpIgDOWzEP5AzqXtCOFYn6RTH5SRug4hKNN7sT1eYMslHu7wtEBDKVgrLjOCe/
W2f8rLT1zEsoAW2ChlZAPYUBkl/0XuTWRg3CohPPcI+UtlRSfvLDeeQ460swjbwgS/RbJh3sIwlCRLU08kEo04Z9H/
AgMBAAECggEAEIeaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/
HlfvCArftGgMaYWPSNCJRMXB7tPwpQu19esjz4Z/
cR2Je4fTLPrffGUsHFgZjv5OQBZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNK
Krciu9YkInNEHu6uRJ5g/eGGX3KQynTvVIhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9MEGpfYI6AdHIwFZcT/
RNAxhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7AlekrguPtfV1vWklg
+bUFhgGaiAEYTpAUN9t2DVIiijgQKBgQDnYMMsaF0r557CM1CTXUqgCZo8MKeV2jf2drlxRRwRl33SksQbzAQ/
qrLdT7GP3sCGqvkxWY2FPdFYf8kxGcCeZPcIeZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/
fbwjpjP7dtJ7n8EzkRUNE6aIMHOFEeych/
PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLriWgTWHXPZxUQaYhpjXo6+lMI6DpExiDgBAkMzJGIvS7y
QiYWU
+wthAr9urbWYdGZlS6VjoTkF6r7VZoILXX0fbuXh6lm8K8IQRfBpJff56p9phMwaBpDNDrfpHB5utBUxs40yIdp6w
KBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zJf3bGSXU/jR4eB1lVQhELGI9CbKSdzKM71GyEImix/
T7FnJSHIWlho1qVo6AQyduNWnAQD15pr8KAdXGXAZZ1FQcb3KYa
+2fflERmazdOTwjYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak/735uP20KKqhNehZpC2dJei7OiIgRhCS/
dKASUXHSW4fptBnUxACYocdDxtY4VhafI7FPMdvGl8ioYbvlHFh+X0Xs9r1S8yeWnHoXMb6eXWmYKMJrAoveLa
+2cFm1Agf7nLhA4R4lqm9IpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAJkD4wHW54Pwd4Ctfk9ojHjWB7pQlUYpT
ZO9dm
+4fpCMn9Okf43AE2yAOaAP94GdzdDJkxfciXKcsYr9IIukfaoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO3
8a5gZaOm/BUlGKMWXzuEd3fy+1rCUwzOp9LSjtJYf4ege-----END PRIVATE KEY-----",
    "certificate" : "-----BEGIN CERTIFICATE-----
MIIC4TCCAcmgAwIBAgICERwDQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXlDb21wYW55IENBMB4X
DTE4MDcwMjEzMjU0N1oXDTQ1MTExNzEzMjU0N1owFDESMBAGA1UEAwwJbG9jYWxob3N0MIIBIjANBgkqh
kiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0FQGzi3ucTX+DNud1p/
b4XVM6I3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5U0NqPQZKUrZz3rQeLN9mYiUTJZPutYlFDDbB8CtlgV
+eyU9yYJslWx/Bm5kWNPh97B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/
W7jaSIAzlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylYKy4zgnv1tn/
Ky09cxLKAFtgoZWQD2FAZJf9F7k1kYNwqITz3CPlLZUUn7yw3nkOOtLMI28IEv0WyYd7CMJQkS1NPJBKNOGfR/
wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29thwQKuUvJhwR/
AAABMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCSqGSIb3DQEBCwUAA4IBAQA8lMQJxaTey7EjXtRLSVl
```

EAMftAQPG6jijNQuvIBQYUDauDT4W2XUZ5wAnjiOyQ83va672K1G9s8n6xlH
+xwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDaezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPR
LYlzp1HMnI6hkjPk4PCZwKnha0dlScati9CCt3UzXSNJOSLalKdHErH08Iqd+1BchScxCfk0xNITn1HZZGmI
+vbmunok3A2lucI14rnsrcbkGYqxGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZiYsGDVN+9QBd0eYUHce
+77s96i3I-----END CERTIFICATE-----",
"admin_state_up" : true,
"created_at" : "2019-04-21T18:59:43Z",
"updated_at" : "2019-04-21T18:59:43Z",
"expire_time" : "2045-11-17T13:25:47Z",
"common_name" : "www.example.com",
"fingerprint" : "869df7fcb441c2ef3fb9329437815972eeb1ef0e",
"subject_alternative_names" : ["www.example.com"]
}, {
"id" : "7875ccb4c6b44cdb90ab2ab89892ab71",
"project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
"name" : "https_certificatekkkk",
"type" : "client",
"domain" : "sda.com",
"description" : "description for certificatehhhh",
"private_key" : "-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDQVAbOLe5xNf4M253Wn9vhdUzojetjv4J
+B7kYwsMhRcgdcJ8KCnX1nfzTvI2ksXlTQ2o9BkpStnPetB4s32ZiJRMlk
+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rMMD30gLh6QoP3cq7PGWcuZKV7hjd1tjCT
QukwMvqV8Icq39buNpIgDOWzEP5AzqXtCOFYn6RTH5SRug4hKNN7sT1eYMslHu7wtEBDKVgrLjOCe/
W2f8rLT1zEsoAW2ChlZAPYUBkl/0XuTWRg3CohPPcI+UtlRSfvLDeeQ460swjbwgS/RbJh3slwlCRLU08kEo04Z9H/
AgMBAAECggEAEIeaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/
HlfvCArftGgMaYWPSNCJRMXB7tPwpQu19esjz4Z/
cR2Je4fTLPrffGUsHFgZjv5OQBZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNK
Krciu9YkInNEHu6uRJ5g/eGGX3KQynTvVIhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9MEGpfYI6AdHIwFZcT/
RNAxhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7AlekrguPtfV1vWklg
+bUFhgGaiAEYTpAUN9t2DVIiijgQKBgQDnYMMsaF0r557CM1CTXUqgCZo8MKeV2jf2drlxRRwRl33SksQbzAQ/
qrLdT7GP3sCGqvkxWY2FPdFYf8kxGcCeZPcIeZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/
fbwjpjP7dtJ7n8EzkRUNE6aIMHOFEeych/
PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLriWgTWHXPZxUQaYhpjXo6+lMI6DpExiDgBAkMzJGIvS7y
QiYWU
+wthAr9urbWYdGZlS6VjoTkF6r7VZoILXX0fbuXh6lm8K8IQRfBpJff56p9phMwaBpDNDrfpHB5utBUxs40yIdp6w
KBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zJf3bGSXU/jR4eB1lVQhELGI9CbKSdzKM71GyEImix/
T7FnJSHIWlho1qVo6AQyduNWnAQD15pr8KAdXGXAZZ1FQcb3KYa
+2fflERmazdOTwjYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak/735uP20KKqhNehZpC2dJei7OiIgRhCS/
dKASUXHSW4fptBnUxACYocdDxtY4VhafI7FPMdvGl8ioYbvlHFh+X0Xs9r1S8yeWnHoXMb6eXWmYKMJrAoveLa
+2cFm1Agf7nLhA4R4lqm9IpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAJkD4wHW54Pwd4Ctfk9ojHjWB7pQlUYpT
ZO9dm
+4fpCMn9Okf43AE2yAOaAP94GdzdDJkxfciXKcsYr9IIukfaoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO3
8a5gZaOm/BUlGKMWXzuEd3fy+1rCUwzOp9LSjtJYf4ege-----END PRIVATE KEY-----",
"certificate" : "-----BEGIN CERTIFICATE-----
MIIC4TCCAcmgAwIBAgICEREwDQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXlDb21wYW55IENBMB4X
DTE4MDcwMjEzMjU0N1oXDTQ1MTExNzEzMjU0N1owFDESMBAGA1UEAwwJbG9jYWxob3N0MIIBIjANBgkqh
kiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0FQGzi3ucTX+DNud1p/
b4XVM6I3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5U0NqPQZKUrZz3rQeLN9mYiUTJZPutYlFDDbB8CtlgV
+eyU9yYJslWx/Bm5kWNPh97B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/
W7jaSIAzlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylYKy4zgnv1tn/
Ky09cxLKAFtgoZWQD2FAZJf9F7k1kYNwqITz3CPlLZUUn7yw3nkOOtLMI28IEv0WyYd7CMJQkS1NPJBKNOGfR/
wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29thwQKuUvJhwR/
AAABMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCSqGSIb3DQEBCwUAA4IBAQA8lMQJxaTey7EjXtRLSVl
EAMftAQPG6jijNQuvIBQYUDauDT4W2XUZ5wAnjiOyQ83va672K1G9s8n6xlH
+xwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDaezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPR
LYlzp1HMnI6hkjPk4PCZwKnha0dlScati9CCt3UzXSNJOSLalKdHErH08Iqd+1BchScxCfk0xNITn1HZZGmI
+vbmunok3A2lucI14rnsrcbkGYqxGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZiYsGDVN+9QBd0eYUHce
+77s96i3I-----END CERTIFICATE-----",
"admin_state_up" : true,
"created_at" : "2018-10-29T20:16:17Z",
"updated_at" : "2019-04-06T21:33:24Z",
"expire_time" : "2045-11-17T13:25:47Z",
"common_name" : "www.example.com",
"fingerprint" : "869df7fcb441c2ef3fb9329437815972eeb1ef0e",
"subject_alternative_names" : ["www.example.com"]
}, {
"id" : "7f41c96223d34ebaa3c8e836b6625ec0",
"project_id" : "99a3fff0d03c428eac3678da6a7d0f24",


```
    "name" : "asdf",
    "type" : "server",
    "domain" : "sda.com",
    "description" : "",
    "private_key" : "-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDQVAbOLe5xNf4M253Wn9vhdUzojetjv4J
+B7kYwsMhRcgdcJ8KCnX1nfzTvI2ksXlTQ2o9BkpStnPetB4s32ZiJRMlk
+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rMMD30gLh6QoP3cq7PGWcuZKV7hjd1tjCT
QukwMvqV8Icq39buNpIgDOWzEP5AzqXtCOFYn6RTH5SRug4hKNN7sT1eYMslHu7wtEBDKVgrLjOCe/
W2f8rLT1zEsoAW2ChlZAPYUBkl/0XuTWRg3CohPPcI+UtlRSfvLDeeQ460swjbwgS/RbJh3slwlCRLU08kEo04Z9H/
AgMBAAECggEAEleaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/
HlfvCArftGgMaYWPSNCJRMXB7tPwpQu19esjz4Z/
cR2Je4fTLPrffGUsHFgZjv5OQBZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNK
Krciu9YkInNEHu6uRJ5g/eGGX3KQynTvVIhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9MEGpfYI6AdHIwFZcT/
RNAxhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7AlekrguPtfV1vWklg
+bUFhgGaiAEYTpAUN9t2DVIiijgQKBgQDnYMMsaF0r557CM1CTXUqgCZo8MKeV2jf2drlxRRwRl33SksQbzAQ/
qrLdT7GP3sCGqvkxWY2FPdFYf8kxGcCeZPcIeZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/
fbwjpjP7dtJ7n8EzkRUNE6aIMHOFEeych/
PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLriWgTWHXPZxUQaYhpjXo6+lMI6DpExiDgBAkMzJGIvS7y
QiYWU
+wthAr9urbWYdGZlS6VjoTkF6r7VZoILXX0fbuXh6lm8K8IQRfBpJff56p9phMwaBpDNDrfpHB5utBUxs40yIdp6w
KBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zJf3bGSXU/jR4eB1lVQhELGI9CbKSdzKM71GyEImix/
T7FnJSHIWlho1qVo6AQyduNWnAQD15pr8KAdXGXAZZ1FQcb3KYa
+2fflERmazdOTwjYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak/735uP20KKqhNehZpC2dJei7OiIgRhCS/
dKASUXHSW4fptBnUxACYocdDxtY4VhafI7FPMdvGl8ioYbvlHFh+X0Xs9r1S8yeWnHoXMb6eXWmYKMJrAoveLa
+2cFm1Agf7nLhA4R4lqm9IpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAJkD4wHW54Pwd4Ctfk9ojHjWB7pQlUYpT
ZO9dm
+4fpCMn9Okf43AE2yAOaAP94GdzdDJkxfciXKcsYr9IIukfaoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO3
8a5gZaOm/BUlGKMWXzuEd3fy+1rCUwzOp9LSjtJYf4ege-----END PRIVATE KEY-----",
    "certificate" : "-----BEGIN CERTIFICATE-----
MIIC4TCCAcmgAwIBAgICEREwDQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXlDb21wYW55IENBMB4X
DTE4MDcwMjEzMjU0N1oXDTQ1MTExNzEzMjU0N1owFDESMBAGA1UEAwwJbG9jYWxob3N0MIIBIjANBgkqh
kiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0FQGzi3ucTX+DNud1p/
b4XVM6I3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5U0NqPQZKUrZz3rQeLN9mYiUTJZPutYlFDDbB8CtlgV
+eyU9yYJslWx/Bm5kWNPh97B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/
W7jaSIAzlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylYKy4zgnv1tn/
Ky09cxLKAFtgoZWQD2FAZJf9F7k1kYNwqITz3CPlLZUUn7yw3nkOOtLMI28IEv0WyYd7CMJQkS1NPJBKNOGfR/
wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29thwQKuUvJhwR/
AAABMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCSqGSIb3DQEBCwUAA4IBAQA8lMQJxaTey7EjXtRLSVl
EAMftAQPG6jijNQuvIBQYUDauDT4W2XUZ5wAnjiOyQ83va672K1G9s8n6xlH
+xwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDaezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPR
LYlzp1HMnI6hkjPk4PCZwKnha0dlScati9CCt3UzXSNJOSLalKdHErH08Iqd+1BchScxCfk0xNITn1HZZGmI
+vbmunok3A2lucI14rnsrcbkGYqxGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZiYsGDVN+9QBd0eYUHce
+77s96i3I-----END CERTIFICATE-----",
    "admin_state_up" : true,
    "created_at" : "2019-03-31T22:23:51Z",
    "updated_at" : "2019-03-31T23:26:49Z",
    "expire_time" : "2045-11-17T13:25:47Z",
    "common_name" : "www.example.com",
    "fingerprint" : "869df7fcb441c2ef3fb9329437815972eeb1ef0e",
    "subject_alternative_names" : [ "www.example.com" ]
  } ],
  "page_info" : {
    "previous_marker" : "5494a835d88f40ff940554992f2f04d4",
    "current_count" : 3
  },
  "request_id" : "a27e7ae6-d901-4ec2-8e66-b8a1413819ad"
}
```


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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ListCertificatesSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ListCertificatesRequest request = new ListCertificatesRequest();
        try {
            ListCertificatesResponse response = client.listCertificates(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListCertificatesRequest()
        response = client.list_certificates(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListCertificatesRequest{}
    response, err := client.ListCertificates(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	Successful request.

Error Codes

See **Error Codes**.

5.7.3 Querying the Details of a Certificate

Function

This API is used to query the details of an SSL certificate.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/certificates/{certificate_id}

Table 5-175 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
certificate_id	Yes	String	Specifies a certificate ID.

Request Parameters

Table 5-176 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-177 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
certificate	CertificateInfo object	Specifies the certificate.

Table 5-178 CertificateInfo

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the certificate. This parameter is unsupported. Please do not use it.
certificate	String	Specifies the certificate content. The value must be PEM encoded.
description	String	Provides supplementary information about the certificate.
domain	String	Specifies the domain names used by the server certificate. This parameter will take effect only when **type** is set to **server**. Note the following when specifying a domain name: • The value can contain 0 to 10,000 characters and consists of multiple common domain names or wildcard domain names separated by commas. A maximum of 100 domain names are allowed. • A common domain name consists of several labels separated by periods (.). Each label can contain a maximum of 63 characters, including letters, digits, and hyphens (-), and must start and end with a letter or digit. Example: www.test.com • A wildcard domain name is a domain name that starts with *. Example: *.test.com
id	String	Specifies the certificate ID.

Parameter	Type	Description
name	String	Specifies the certificate name.
private_key	String	Specifies the private key of the certificate used by HTTPS listeners. The value must be PEM encoded characters. • This parameter will be ignored even if **type** is set to **client**. The certificate can still be created and used normally. • This parameter is valid and mandatory only when **type** is set to **server**.
type	String	Specifies the certificate type. The value can be **server** or **client**. **server** indicates server certificates, and **client** indicates CA certificates. The default value is **server**.
created_at	String	Specifies the time when the certificate was created.
updated_at	String	Specifies the time when the certificate was updated.
expire_time	String	Specifies the time when the certificate expires.
project_id	String	Specifies the project ID of the certificate.
enc_certificate	String	Specifies the body of the SM encryption certificate required by HTTPS listeners. The value must be PEM encoded. Note: This parameter is returned only when the SM encryption certificate feature is enabled at the site.
enc_private_key	String	Specifies the private key of the SM encryption certificate required by HTTPS listeners. The value must be PEM encoded. Note: This parameter is returned only when the SM encryption certificate feature is enabled at the site.
scm_certificate_id	String	Specifies the SSL certificate ID.
common_name	String	Specifies the primary domain name of the certificate.

Parameter	Type	Description
fingerprint	String	Specifies the fingerprint of the certificate.
subject_alternative_names	Array of strings	Specifies all the domain names of the certificate.

Example Requests

Querying the details of a certificate

```
GET https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/certificates/
5494a835d88f40ff940554992f2f04d4
```

Example Responses

Status code: 200

Successful request.


```
{
  "certificate" : {
    "id" : "5494a835d88f40ff940554992f2f04d4",
    "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
    "name" : "https_certificatekkkk",
    "type" : "server",
    "domain" : null,
    "description" : "description for certificatehhhh",
    "private_key" : "-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDQVAbOLe5xNf4M253Wn9vhdUzojetjv4J
+B7kYwsMhRcgdcJ8KCnX1nfzTvI2ksXlTQ2o9BkpStnPetB4s32ZiJRMlk
+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rMMD30gLh6QoP3cq7PGWcuZKV7hjd1tjCT
QukwMvqV8Icq39buNpIgDOWzEP5AzqXtCOFYn6RTH5SRug4hKNN7sT1eYMslHu7wtEBDKVgrLjOCe/
W2f8rLT1zEsoAW2ChlZAPYUBkl/0XuTWRg3CohPPcI+UtlRSfvLDeeQ460swjbwgS/RbJh3sIwlCRLU08kEo04Z9H/
AgMBAAECggEAEIeaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/
HlfvCArftGgMaYWPSNCJRMXB7tPwpQu19esjz4Z/
cR2Je4fTLPrffGUsHFgZjv5OQBZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNK
Krciu9YkInNEHu6uRJ5g/eGGX3KQynTvVlhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9MEGpfYI6AdHIwFZcT/
RNAxhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7AlekrguPtfV1vWklg
+bUFhgGaiAEYTpAUN9t2DVIiijgQKBgQDnYMMsaF0r557CM1CTXUqgCZo8MKeV2jf2drlxRRwRl33SksQbzAQ/
qrLdT7GP3sCGqvkxWY2FPdFYf8kxGcCeZPcIeZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/
fbwjpjP7dtJ7n8EzkRUNE6aIMHOFEeych/
PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLriWgTWHXPZxUQaYhpjXo6+lMI6DpExiDgBAkMzJGIvS7y
QiYWU
+wthAr9urbWYdGZlS6VjoTkF6r7VZoILXX0fbuXh6lm8K8IQRfBpJff56p9phMwaBpDNDrfpHB5utBUxs40yIdp6w
KBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zJf3bGSXU/jR4eB1lVQhELGI9CbKSdzKM71GyEImix/
T7FnJSHIWlho1qVo6AQyduNWnAQD15pr8KAdXGXAZZ1FQcb3KYa
+2fflERmazdOTwjYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak/735uP20KKqhNehZpC2dJei7OiIgRhCS/
dKASUXHSW4fptBnUxACYocdDxtY4VhafI7FPMdvGl8ioYbvlHFh+X0Xs9r1S8yeWnHoXMb6eXWmYKMJrAoveLa
+2cFm1Agf7nLhA4R4lqm9IpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAJkD4wHW54Pwd4Ctfk9ojHjWB7pQlUYpT
ZO9dm
+4fpCMn9Okf43AE2yAOaAP94GdzdDJkxfciXKcsYr9IIukfaoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO3
8a5gZaOm/BUlGKMWXzuEd3fy+1rCUwzOp9LSjtJYf4ege-----END PRIVATE KEY-----",
    "certificate" : "-----BEGIN CERTIFICATE-----
MIIC4TCCAcmgAwIBAgICEREwDQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXlDb21wYW55IENBMB4X
DTE4MDcwMjEzMjU0N1oXDTQ1MTExNzEzMjU0N1owFDESMBAGA1UEAwwJbG9jYWxob3N0MIIBIjANBgkqh
kiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0FQGzi3ucTX+DNud1p/
b4XVM6I3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5U0NqPQZKUrZz3rQeLN9mYiUTJZPutYlFDDbB8CtlgV
+eyU9yYJslWx/Bm5kWNPh97B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/
W7jaSIAzlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylYKy4zgnv1tn/
Ky09cxLKAFtgoZWQD2FAZJf9F7k1kYNwqITz3CPlLZUUn7yw3nkOOtLMI28IEv0WyYd7CMJQkS1NPJBKNOGfR/
wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29thwQKuUvJhwR/
```


AAABMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCSqGSIb3DQEBCwUAA4IBAQA8lMQJxaTey7EjXtRLSVl
EAMftAQPG6jijNQuvIBQYUDauDT4W2XUZ5wAnjiOyQ83va672K1G9s8n6xlH
+xwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDaezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPR
LYlzp1HMnI6hkjPk4PCZwKnha0dlScati9CCt3UzXSNJOSLalKdHErH08Iqd+1BchScxCfk0xNITn1HZZGmI
+vbmunok3A2lucI14rnsrcbkGYqxGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZiYsGDVN+9QBd0eYUHce
+77s96i3I-----END CERTIFICATE-----",
    "admin_state_up" : true,
    "created_at" : "2019-03-31T22:23:51Z",
    "updated_at" : "2019-03-31T23:26:49Z",
    "expire_time" : "2045-11-17T13:25:47Z",
    "common_name" : "www.example.com",
    "fingerprint" : "869df7fcb441c2ef3fb9329437815972eeb1ef0e",
    "subject_alternative_names" : ["www.example.com"]
  },
  "request_id" : "a94af450-5ac0-4185-946c-27a59a16c1d3"
}

Status Codes

Status Code	Description
200	Successful request.

Error Codes

See **Error Codes**.

5.7.4 Updating a Certificate

Function

This API is used to update an SSL certificate.

Constraints

If a certificate with a domain name is used by a listener, the domain name cannot be updated to an empty string (""), and the system returns the 409 Conflict status code.

Calling Method

For details, see **Calling APIs**.

URI

PUT /v3/{project_id}/elb/certificates/{certificate_id}

Table 5-179 Path Parameters

Parameter	Mandatory	Type	Description
certificate_id	Yes	String	Specifies a certificate ID.

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID of the certificate.

Request Parameters

Table 5-180 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Table 5-181 Request body parameters

Parameter	Mandatory	Type	Description
certificate	Yes	**UpdateCertificateOption** object	Specifies the certificate.

Table 5-182 UpdateCertificateOption

Parameter	Mandatory	Type	Description
certificate	No	String	Specifies the private key of the certificate. The value must be PEM encoded. Maximum 65,536-character length is allowed, supports certificate chains with a maximum of 11 layers (including certificates and certificate chains).
description	No	String	Provides supplementary information about the certificate.
name	No	String	Specifies the certificate name.

Parameter	Mandatory	Type	Description
private_key	No	String	Specifies the private key of the server certificate. The value must be PEM encoded. Maximum 8,192-character length is allowed. • This parameter is valid and mandatory only when **type** is set to **server**. • This parameter will not take effect and an error will be returned if **type** is set to **client**.
domain	No	String	Specifies the domain names used by the server certificate. This parameter will take effect only when **type** is set to **server**. Note the following when specifying a domain name: • The value can contain 0 to 10,000 characters and consists of multiple common domain names or wildcard domain names separated by commas. A maximum of 100 domain names are allowed. • A common domain name consists of several labels separated by periods (.). Each label can contain a maximum of 63 characters, including letters, digits, and hyphens (-), and must start and end with a letter or digit. Example: www.test.com • A wildcard domain name is a domain name that starts with *. Example: *.test.com

Parameter	Mandatory	Type	Description
enc_certificate	No	String	Specifies the body of the SM encryption certificate required by HTTPS. The value must be PEM encoded. Maximum 65,536-character length is allowed, supports certificate chains with a maximum of 11 layers (including certificates and certificate chains). This parameter is mandatory only when **type** is set to **server_sm**.
enc_private_key	No	String	Specifies the body of the SM encryption certificate required by HTTPS. The value must be PEM encoded. Maximum 8,192-character length is allowed. This parameter is mandatory only when **type** is set to **server_sm**.
scm_certificate_id	No	String	Specifies the SCM certificate ID.

Response Parameters

Status code: 200

Table 5-183 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
certificate	**CertificateInfo** object	Specifies the certificate.

Table 5-184 CertificateInfo

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the certificate. This parameter is unsupported. Please do not use it.
certificate	String	Specifies the certificate content. The value must be PEM encoded.
description	String	Provides supplementary information about the certificate.
domain	String	Specifies the domain names used by the server certificate. This parameter will take effect only when **type** is set to **server**. Note the following when specifying a domain name: • The value can contain 0 to 10,000 characters and consists of multiple common domain names or wildcard domain names separated by commas. A maximum of 100 domain names are allowed. • A common domain name consists of several labels separated by periods (.). Each label can contain a maximum of 63 characters, including letters, digits, and hyphens (-), and must start and end with a letter or digit. Example: www.test.com • A wildcard domain name is a domain name that starts with *. Example: *.test.com
id	String	Specifies the certificate ID.
name	String	Specifies the certificate name.

Parameter	Type	Description
private_key	String	Specifies the private key of the certificate used by HTTPS listeners. The value must be PEM encoded characters. • This parameter will be ignored even if **type** is set to **client**. The certificate can still be created and used normally. • This parameter is valid and mandatory only when **type** is set to **server**.
type	String	Specifies the certificate type. The value can be **server** or **client**. **server** indicates server certificates, and **client** indicates CA certificates. The default value is **server**.
created_at	String	Specifies the time when the certificate was created.
updated_at	String	Specifies the time when the certificate was updated.
expire_time	String	Specifies the time when the certificate expires.
project_id	String	Specifies the project ID of the certificate.
enc_certificate	String	Specifies the body of the SM encryption certificate required by HTTPS listeners. The value must be PEM encoded. Note: This parameter is returned only when the SM encryption certificate feature is enabled at the site.
enc_private_key	String	Specifies the private key of the SM encryption certificate required by HTTPS listeners. The value must be PEM encoded. Note: This parameter is returned only when the SM encryption certificate feature is enabled at the site.
scm_certificate_id	String	Specifies the SSL certificate ID.
common_name	String	Specifies the primary domain name of the certificate.

Parameter	Type	Description
fingerprint	String	Specifies the fingerprint of the certificate.
subject_alternative_names	Array of strings	Specifies all the domain names of the certificate.

Example Requests

Modifying the name and description of a certificate

```
PUT https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/certificates/
233a325e5e3e4ce8beeb320aa714cc12

{
  "certificate" : {
    "name" : "My Certificate",
    "description" : "Update my Certificate."
  }
}
```

Example Responses

Status code: 200

Successful request.

```
{
  "certificate" : {
    "private_key" : "-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDQVAbOLe5xNf4M253Wn9vhdUzojetjv4J
+B7kYwsMhRcgdcJ8KCnX1nfzTvI2ksXlTQ2o9BkpStnPetB4s32ZiJRMlk
+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rMMD30gLh6QoP3cq7PGWcuZKV7hjd1tjCT
QukwMvqV8Icq39buNpIgDOWzEP5AzqXtCOFYn6RTH5SRug4hKNN7sT1eYMslHu7wtEBDKVgrLjOCe/
W2f8rLT1zEsoAW2ChlZAPYUBkl/0XuTWRg3CohPPcI+UtlRSfvLDeeQ460swjbwgS/RbJh3sIwlCRLU08kEo04Z9H/
AgMBAAECggEAEIeaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/
HlfvCArftGgMaYWPSNCJRMXB7tPwpQu19esjz4Z/
cR2Je4fTLPrffGUsHFgZjv5OQBZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNK
Krciu9YkInNEHu6uRJ5g/eGGX3KQynTvVIhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9MEGpfYI6AdHIwFZcT/
RNAxhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7AlekrguPtfV1vWklg
+bUFhgGaiAEYTpAUN9t2DVIiijgQKBgQDnYMMsaF0r557CM1CTXUqgCZo8MKeV2jf2drlxRRwRl33SksQbzAQ/
qrLdT7GP3sCGqvkxWY2FPdFYf8kxGcCeZPcIeZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/
fbwjpjP7dtJ7n8EzkRUNE6aIMHOFEeych/
PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLriWgTWHXPZxUQaYhpjXo6+lMI6DpExiDgBAkMzJGIvS7y
QiYWU
+wthAr9urbWYdGZlS6VjoTkF6r7VZoILXX0fbuXh6lm8K8IQRfBpJff56p9phMwaBpDNDrfpHB5utBUxs40yIdp6w
KBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zJf3bGSXU/jR4eB1lVQhELGI9CbKSdzKM71GyEImix/
T7FnJSHIWlho1qVo6AQyduNWnAQD15pr8KAdXGXAZZ1FQcb3KYa
+2ffIERmazdOTwjYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak/735uP20KKqhNehZpC2dJei7OiIgRhCS/
dKASUXHSW4fptBnUxACYocdDxtY4VhafI7FPMdvGl8ioYbvlHFh+X0Xs9r1S8yeWnHoXMb6eXWmYKMJrAoveLa
+2cFm1Agf7nLhA4R4lqm9IpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAJkD4wHW54Pwd4Ctfk9ojHjWB7pQlUYpT
ZO9dm
+4fpCMn9Okf43AE2yAOaAP94GdzdDJkxfciXKcsYr9IIukfaoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO3
8a5gZaOm/BUlGKMWXzuEd3fy+1rCUwzOp9LSjtJYf4ege-----END PRIVATE KEY-----",
    "description" : "Update my Certificate.",
    "domain" : null,
    "created_at" : "2019-03-31T22:23:51Z",
    "expire_time" : "2045-11-17T13:25:47Z",
    "id" : "233a325e5e3e4ce8beeb320aa714cc12",
    "name" : "My Certificate",
    "certificate" : "-----BEGIN CERTIFICATE-----
MIIC4TCCAcmgAwIBAgICEREwDQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXlDb21wYW55IENBMB4X
```


DTE4MDcwMjEzMjU0N1oXDTQ1MTExNzEzMjU0N1owFDESMBAGA1UEAwwJbG9jYWxob3N0MIIBIjANBgkqh
kiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0FQGzi3ucTX+DNud1p/
b4XVM6I3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5U0NqPQZKUrZz3rQeLN9mYiUTJZPutYlFDDbB8CtlgV
+eyU9yYJslWx/Bm5kWNPh97B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/
W7jaSIAzlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylYKy4zgnv1tn/
Ky09cxLKAFtgoZWQD2FAZJf9F7k1kYNwqITz3CPlLZUUn7yw3nkOOtLMI28IEv0WyYd7CMJQkS1NPJBKNOGfR/
wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29thwQKuUvJhwR/
AAABMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCSqGSIb3DQEBCwUAA4IBAQA8lMQJxaTey7EjXtRLSVl
EAMftAQPG6jijNQuvIBQYUDauDT4W2XUZ5wAnjiOyQ83va672K1G9s8n6xlH
+xwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDaezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPR
LYlzp1HMnI6hkjPk4PCZwKnha0dlScati9CCt3UzXSNJOSLalKdHErH08Iqd+1BchScxCfk0xNITn1HZZGmI
+vbmunok3A2lucI14rnsrcbkGYqxGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZiYsGDVN+9QBd0eYUHce
+77s96i3I-----END CERTIFICATE-----",
    "admin_state_up" : true,
    "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
    "updated_at" : "2019-03-31T23:26:49Z",
    "type" : "server",
    "common_name" : "www.example.com",
    "fingerprint" : "869df7fcb441c2ef3fb9329437815972eeb1ef0e",
    "subject_alternative_names" : ["www.example.com"]
  },
  "request_id" : "d9abea6b-98ee-4ad4-8c5d-185ded48742f"
}

SDK Sample Code

The SDK sample code is as follows.

Java

Modifying the name and description of a certificate

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class UpdateCertificateSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdateCertificateRequest request = new UpdateCertificateRequest();
        request.withCertificateId("{certificate_id}");
```



```
        UpdateCertificateRequestBody body = new UpdateCertificateRequestBody();
        UpdateCertificateOption certificatebody = new UpdateCertificateOption();
        certificatebody.withDescription("Update my Certificate.")
            .withName("My Certificate");
        body.withCertificate(certificatebody);
        request.withBody(body);
        try {
            UpdateCertificateResponse response = client.updateCertificate(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

Modifying the name and description of a certificate

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdateCertificateRequest()
        request.certificate_id = "{certificate_id}"
        certificatebody = UpdateCertificateOption(
            description="Update my Certificate.",
            name="My Certificate"
        )
        request.body = UpdateCertificateRequestBody(
            certificate=certificatebody
        )
        response = client.update_certificate(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

Modifying the name and description of a certificate

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdateCertificateRequest{}
    request.CertificateId = "{certificate_id}"
    descriptionCertificate:= "Update my Certificate."
    nameCertificate:= "My Certificate"
    certificatebody := &model.UpdateCertificateOption{
        Description: &descriptionCertificate,
        Name: &nameCertificate,
    }
    request.Body = &model.UpdateCertificateRequestBody{
        Certificate: certificatebody,
    }
    response, err := client.UpdateCertificate(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	Successful request.

Error Codes

See **Error Codes**.

5.7.5 Deleting a Certificate

Function

This API is used to delete an SSL certificate.

Constraints

If the certificate is used by a listener, the certificate cannot be deleted, and the 409 Conflict error code will be displayed.

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v3/{project_id}/elb/certificates/{certificate_id}

Table 5-185 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
certificate_id	Yes	String	Specifies a certificate ID.

Request Parameters

Table 5-186 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

None

Example Requests

Deleting an SSL certificate

```
DELETE https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/certificates/
233a325e5e3e4ce8beeb320aa714cc12
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class DeleteCertificateSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteCertificateRequest request = new DeleteCertificateRequest();
        request.withCertificateId("{certificate_id}");
        try {
            DeleteCertificateResponse response = client.deleteCertificate(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteCertificateRequest()
        request.certificate_id = "{certificate_id}"
        response = client.delete_certificate(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteCertificateRequest{}
    request.CertificateId = "{certificate_id}"
    response, err := client.DeleteCertificate(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	Successful request.

Error Codes

See **Error Codes**.

5.7.6 Enabling or Disabling the Private Key Feature

Function

This API is used to enable or disable **private-key-echo**.

Calling Method

For details, see **Calling APIs**.

URI

POST /v3/{project_id}/elb/certificates/settings/private-key-echo

Table 5-187 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Request Parameters

Table 5-188 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Table 5-189 Request body parameters

Parameter	Mandatory	Type	Description
private_key_echo	Yes	Boolean	Specifies whether to enable **private_key_echo**. The default value is **true**, indicating that the private key is displayed in the response body. This parameter takes effect by project ID. If the value is set to **false**, the private key is not displayed in the response body.

Response Parameters

Status code: 201

Table 5-190 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.

Parameter	Type	Description
private_key_echo	Boolean	Specifies whether **private_key_echo** is enabled. The default value is **true**, indicating that the private key is displayed in the response body. This parameter takes effect by project ID. If the value is set to **false**, the private key is not displayed in the response body.

Example Requests

Enabling or disabling the private key feature

```
POST https://{ELB_Endpoint}/v3/{project_id}/elb/certificates/settings/private-key-echo

{
  "private_key_echo" : true
}
```

Example Responses

Status code: 201

Normal response code for POST operations

```
{
  "private_key_echo" : true,
  "request_id" : "98414965-856c-4be3-8a33-3e08432a222e"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Enabling or disabling the private key feature

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class CreateCertificatePrivateKeyEchoSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateCertificatePrivateKeyEchoRequest request = new CreateCertificatePrivateKeyEchoRequest();
        CreateCertificatePrivateKeyEchoRequestBody body = new
CreateCertificatePrivateKeyEchoRequestBody();
        body.withPrivateKeyEcho(true);
        request.withBody(body);
        try {
            CreateCertificatePrivateKeyEchoResponse response = client.createCertificatePrivateKeyEcho(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

Enabling or disabling the private key feature

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateCertificatePrivateKeyEchoRequest()
        request.body = CreateCertificatePrivateKeyEchoRequestBody(
            private_key_echo=True
```



```
        )
        response = client.create_certificate_private_key_echo(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

Enabling or disabling the private key feature

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateCertificatePrivateKeyEchoRequest{}
    request.Body = &model.CreateCertificatePrivateKeyEchoRequestBody{
        PrivateKeyEcho: true,
    }
    response, err := client.CreateCertificatePrivateKeyEcho(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 code for POST operations

Error Codes

See **Error Codes**.

5.7.7 Querying Whether the Private Key Feature Is Enabled

Function

This API is used to query whether **private-key-echo** is set to **true** or **false**.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/certificates/settings/private-key-echo

Table 5-191 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Request Parameters

Table 5-192 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-193 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
private_key_echo	Boolean	Specifies whether **private_key_echo** is enabled. The default value is **true**, indicating that the private key is displayed in the response body. This parameter takes effect by project ID. If the value is set to **false**, the private key is not displayed in the response body.

Example Requests

Querying whether the private key feature is enabled

```
GET https://{ELB_Endpoint}/v3/{project_id}/elb/certificates/settings/private-key-echo
```

Example Responses

Status code: 200

Normal response code for GET operations

```
{
  "private_key_echo" : true,
  "request_id" : "98414965-856c-4be3-8a33-3e08432a222e"
}
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ShowCertificatePrivateKeyEchoSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowCertificatePrivateKeyEchoRequest request = new ShowCertificatePrivateKeyEchoRequest();
        try {
            ShowCertificatePrivateKeyEchoResponse response = client.showCertificatePrivateKeyEcho(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowCertificatePrivateKeyEchoRequest()
        response = client.show_certificate_private_key_echo(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowCertificatePrivateKeyEchoRequest{}
    response, err := client.ShowCertificatePrivateKeyEcho(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 code for GET operations

Error Codes

See **Error Codes**.

5.8 Security Policy

5.8.1 Creating a Custom Security Policy

Function

This API is used to create a custom security policy. If you need a custom security policy, you need to specify **security_policy_id** when you add an HTTPS listener to your load balancer.

Calling Method

For details, see **Calling APIs**.

URI

POST /v3/{project_id}/elb/security-policies

Table 5-194 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Request Parameters

Table 5-195 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Table 5-196 Request body parameters

Parameter	Mandatory	Type	Description
security_policy	Yes	**CreateSecurityPolicyOption** object	Specifies the custom security policy.

Table 5-197 CreateSecurityPolicyOption

Parameter	Mandatory	Type	Description
name	No	String	Specifies the name of the custom security policy. The default value is "".

Parameter	Mandatory	Type	Description
description	No	String	Provides supplementary information about the custom security policy. The default value is "".
enterprise_project_id	No	String	Specifies the enterprise project ID.
protocols	Yes	Array of strings	Lists the TLS protocols supported by the custom security policy. Value options: **TLSv1**, **TLSv1.1**, **TLSv1.2**, and **TLSv1.3**.

Parameter	Mandatory	Type	Description
ciphers	Yes	Array of strings	Lists the cipher suites supported by the custom security policy. The following cipher suites are supported: ECDHE-RSA-AES256-GCM-SHA384,ECDHE-RSA-AES128-GCM-SHA256,ECDHE-ECDSA-AES256-GCM-SHA384,ECDHE-ECDSA-AES128-GCM-SHA256,AES128-GCM-SHA256,AES256-GCM-SHA384,ECDHE-ECDSA-AES128-SHA256,ECDHE-RSA-AES128-SHA256,AES128-SHA256,AES256-SHA256,ECDHE-ECDSA-AES256-SHA384,ECDHE-RSA-AES256-SHA384,ECDHE-ECDSA-AES128-SHA,ECDHE-RSA-AES128-SHA,ECDHE-RSA-AES256-SHA,ECDHE-ECDSA-AES256-SHA,AES128-SHA,AES256-SHA,CAMELLIA128-SHA,DES-CBC3-SHA,CAMELLIA256-SHA,ECDHE-RSA-CHACHA20-POLY1305,ECDHE-ECDSA-CHACHA20-POLY1305,TLS_AES_128_GCM_SHA256,TLS_AES_256_GCM_SHA384,TLS_CHACHA20_POLY1305_SHA256,TLS_AES_128_CCM_SHA256,TLS_AES_128_CCM_8_SHA256 Note: • The protocol and cipher suite must match. At least one cipher suite must match the protocol. • You can match the protocol and cipher suite based on system security policy.

Response Parameters

Status code: 201

Table 5-198 Response body parameters

Parameter	Type	Description
security_policy	**SecurityPolicy** object	Lists the security policies.
request_id	String	Specifies the request ID. Note: The value is automatically generated.

Table 5-199 SecurityPolicy

Parameter	Type	Description
id	String	Specifies the ID of the custom security policy.
project_id	String	Specifies the project ID of the custom security policy.
name	String	Specifies the name of the custom security policy.
description	String	Provides supplementary information about the custom security policy.
listeners	Array of **ListenerRef** objects	Specifies the listeners that use the custom security policies.
protocols	Array of strings	Lists the TLS protocols supported by the custom security policy.
ciphers	Array of strings	Lists the cipher suites supported by the custom security policy.
created_at	String	Specifies the time when the custom security policy was created.
updated_at	String	Specifies the time when the custom security policy was updated.

Table 5-200 ListenerRef

Parameter	Type	Description
id	String	Specifies the listener ID.

Example Requests

Creating a custom security policy and specifying the TLS protocol and cipher suite


```
POST https://{ELB_Endpoint}/v3/7a9941d34fc1497d8d0797429ecfd354/elb/security-policies

{
  "security_policy" : {
    "name" : "test_1",
    "description" : "test1",
    "protocols" : [ "TLSv1.2", "TLSv1", "TLSv1.3" ],
    "ciphers" : [ "ECDHE-ECDSA-AES128-SHA", "TLS_AES_128_GCM_SHA256",
"TLS_AES_128_CCM_8_SHA256" ]
  }
}
```

Example Responses

Status code: 201

Normal response to POST requests.

```
{
  "request_id" : "6b50d914-41f2-4e50-8929-e8a9837dbe75",
  "security_policy" : {
    "id" : "d74e27c9-4d60-427c-a11f-21142117c433",
    "name" : "test_1",
    "project_id" : "7a9941d34fc1497d8d0797429ecfd354",
    "description" : "test1",
    "protocols" : [ "TLSv1.2", "TLSv1", "TLSv1.3" ],
    "ciphers" : [ "ECDHE-ECDSA-AES128-SHA", "TLS_AES_128_GCM_SHA256",
"TLS_AES_128_CCM_8_SHA256" ],
    "listeners" : [ ],
    "created_at" : "2021-03-26T01:33:12Z",
    "updated_at" : "2021-03-26T01:33:12Z"
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Creating a custom security policy and specifying the TLS protocol and cipher suite

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;

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

public class CreateSecurityPolicySolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateSecurityPolicyRequest request = new CreateSecurityPolicyRequest();
        CreateSecurityPolicyRequestBody body = new CreateSecurityPolicyRequestBody();
        List<CreateSecurityPolicyOption.CiphersEnum> listSecurityPolicyCiphers = new ArrayList<>();
        listSecurityPolicyCiphers.add(CreateSecurityPolicyOption.CiphersEnum.fromValue("ECDHE-ECDSA-
AES128-SHA"));

listSecurityPolicyCiphers.add(CreateSecurityPolicyOption.CiphersEnum.fromValue("TLS_AES_128_GCM_SHA2
56"));

listSecurityPolicyCiphers.add(CreateSecurityPolicyOption.CiphersEnum.fromValue("TLS_AES_128_CCM_8_SHA
256"));
        List<String> listSecurityPolicyProtocols = new ArrayList<>();
        listSecurityPolicyProtocols.add("TLSv1.2");
        listSecurityPolicyProtocols.add("TLSv1");
        listSecurityPolicyProtocols.add("TLSv1.3");
        CreateSecurityPolicyOption securityPolicybody = new CreateSecurityPolicyOption();
        securityPolicybody.withName("test_1")
            .withDescription("test1")
            .withProtocols(listSecurityPolicyProtocols)
            .withCiphers(listSecurityPolicyCiphers);
        body.withSecurityPolicy(securityPolicybody);
        request.withBody(body);
        try {
            CreateSecurityPolicyResponse response = client.createSecurityPolicy(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

Creating a custom security policy and specifying the TLS protocol and cipher suite

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateSecurityPolicyRequest()
        listCiphersSecurityPolicy = [
            "ECDHE-ECDSA-AES128-SHA",
            "TLS_AES_128_GCM_SHA256",
            "TLS_AES_128_CCM_8_SHA256"
        ]
        listProtocolsSecurityPolicy = [
            "TLSv1.2",
            "TLSv1",
            "TLSv1.3"
        ]
        securityPolicybody = CreateSecurityPolicyOption(
            name="test_1",
            description="test1",
            protocols=listProtocolsSecurityPolicy,
            ciphers=listCiphersSecurityPolicy
        )
        request.body = CreateSecurityPolicyRequestBody(
            security_policy=securityPolicybody
        )
        response = client.create_security_policy(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

Creating a custom security policy and specifying the TLS protocol and cipher suite

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateSecurityPolicyRequest{}
    var listCiphersSecurityPolicy = []model.CreateSecurityPolicyOptionCiphers{
        model.GetCreateSecurityPolicyOptionCiphersEnum().ECDHE_ECDSA_AES128_SHA,
        model.GetCreateSecurityPolicyOptionCiphersEnum().TLS_AES_128_GCM_SHA256,
        model.GetCreateSecurityPolicyOptionCiphersEnum().TLS_AES_128_CCM_8_SHA256,
    }
    var listProtocolsSecurityPolicy = []string{
        "TLSv1.2",
        "TLSv1",
        "TLSv1.3",
    }
    nameSecurityPolicy:= "test_1"
    descriptionSecurityPolicy:= "test1"
    securityPolicybody := &model.CreateSecurityPolicyOption{
        Name: &nameSecurityPolicy,
        Description: &descriptionSecurityPolicy,
        Protocols: listProtocolsSecurityPolicy,
        Ciphers: listCiphersSecurityPolicy,
    }
    request.Body = &model.CreateSecurityPolicyRequestBody{
        SecurityPolicy: securityPolicybody,
    }
    response, err := client.CreateSecurityPolicy(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 POST requests.

Error Codes

See **Error Codes**.

5.8.2 Querying Custom Security Policies

Function

This API is used to query custom security policies.

Constraints

This API has the following constraints:

- Parameters **marker**, **limit**, and **page_reverse** are used for pagination query.
- Parameters **marker** and **page_reverse** take effect only when they are used together with parameter **limit**.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/security-policies

Table 5-201 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Table 5-202 Query Parameters

Parameter	Mandatory	Type	Description
marker	No	String	Specifies the ID of the last record on the previous page. Note: • This parameter must be used together with **limit**. • If this parameter is not specified, the first page will be queried. • This parameter cannot be left blank or set to an invalid ID.
limit	No	Integer	Specifies the number of records on each page. Value range: 0–2000 Default value: 2000

Parameter	Mandatory	Type	Description
page_reverse	No	Boolean	Specifies whether to use reverse query. Value options: • **true**: Query the previous page. • **false** (default): Query the next page. Note: • This parameter must be used together with **limit**. • If **page_reverse** is set to **true** and you want to query the previous page, set the value of **marker** to the value of **previous_marker**.
id	No	Array of strings	Specifies the ID of the custom security policy. Multiple IDs can be queried in the format of *id=xxx&id=xxx*.
name	No	Array of strings	Specifies the name of the custom security policy. Multiple names can be queried in the format of *name=xxx&name=xxx*.
description	No	Array of strings	Provides supplementary information about the custom security policy. Multiple descriptions can be queried in the format of *description=xxx&description=xxx*.
protocols	No	Array of strings	Specifies the TLS protocols supported by the custom security policy. (Multiple protocols are separated using spaces.) Multiple protocols can be queried in the format of *protocols=xxx&protocols=xxx*.

Parameter	Mandatory	Type	Description
ciphers	No	Array of strings	Specifies the cipher suites supported by the custom security policy. (Multiple cipher suites are separated using colons.) Multiple cipher suites can be queried in the format of *ciphers=xxx&ciphers=xxx*.

Request Parameters

Table 5-203 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-204 Response body parameters

Parameter	Type	Description
security_policies	Array of **SecurityPolicy** objects	Lists the security policies.
request_id	String	Specifies the request ID. Note: The value is automatically generated.
page_info	**PageInfo** object	Shows pagination information.

Table 5-205 SecurityPolicy

Parameter	Type	Description
id	String	Specifies the ID of the custom security policy.
project_id	String	Specifies the project ID of the custom security policy.

Parameter	Type	Description
name	String	Specifies the name of the custom security policy.
description	String	Provides supplementary information about the custom security policy.
listeners	Array of **ListenerRef** objects	Specifies the listeners that use the custom security policies.
protocols	Array of strings	Lists the TLS protocols supported by the custom security policy.
ciphers	Array of strings	Lists the cipher suites supported by the custom security policy.
created_at	String	Specifies the time when the custom security policy was created.
updated_at	String	Specifies the time when the custom security policy was updated.

Table 5-206 ListenerRef

Parameter	Type	Description
id	String	Specifies the listener ID.

Table 5-207 PageInfo

Parameter	Type	Description
previous_marker	String	Specifies the ID of the first record in the pagination query result. When **page_reverse** is set to **true**, this parameter is used together to query resources on the previous page.
next_marker	String	Specifies the ID of the last record in the pagination query result.
current_count	Integer	Specifies the number of records.

Example Requests

Querying custom security policies on each page

```
GET https://{ELB_Endpoint}/v3/7a9941d34fc1497d8d0797429ecfd354/elb/security-policies?limit=2
```


Example Responses

Status code: 200

Successful request.


```
{
  "request_id" : "88424a61-6fa1-4850-aa8b-ce31d78abcf2",
  "security_policies" : [ {
    "id" : "03cf511a-d130-445e-9b02-12d7049ddabf",
    "name" : "test_security_policy",
    "project_id" : "7a9941d34fc1497d8d0797429ecfd354",
    "description" : "",
    "protocols" : [ "TLSv1", "TLSv1.3" ],
    "ciphers" : [ "AES128-SHA", "TLS_AES_128_GCM_SHA256", "TLS_AES_256_GCM_SHA384",
"TLS_CHACHA20_POLY1305_SHA256", "TLS_AES_128_CCM_SHA256", "TLS_AES_128_CCM_8_SHA256" ],
    "listeners" : [ {
      "id" : "6f7c0d75-81c4-4735-87a0-dc5df0f27f5a"
    } ],
    "created_at" : "2021-02-06T10:07:10Z",
    "updated_at" : "2021-02-06T10:07:10Z"
  }, {
    "id" : "04e5d426-628c-42db-867c-fcaefbed2cab",
    "name" : "update_securitypolicy",
    "project_id" : "7a9941d34fc1497d8d0797429ecfd354",
    "description" : "",
    "protocols" : [ "TLSv1.2", "TLSv1.1", "TLSv1.3" ],
    "ciphers" : [ "CAMELLIA128-SHA", "TLS_AES_256_GCM_SHA384", "TLS_CHACHA20_POLY1305_SHA256",
"TLS_AES_128_CCM_SHA256", "TLS_AES_128_CCM_8_SHA256" ],
    "listeners" : [ {
      "id" : "e19b7379-807e-47fb-b53d-46aff540580c"
    } ],
    "created_at" : "2021-02-06T10:01:58Z",
    "updated_at" : "2021-03-20T07:18:59Z"
  } ],
  "page_info" : {
    "next_marker" : "04e5d426-628c-42db-867c-fcaefbed2cab",
    "previous_marker" : "03cf511a-d130-445e-9b02-12d7049ddabf",
    "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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ListSecurityPoliciesSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ListSecurityPoliciesRequest request = new ListSecurityPoliciesRequest();
        try {
            ListSecurityPoliciesResponse response = client.listSecurityPolicies(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListSecurityPoliciesRequest()
        response = client.list_security_policies(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListSecurityPoliciesRequest{}
    response, err := client.ListSecurityPolicies(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	Successful request.

Error Codes

See **Error Codes**.

5.8.3 Querying the Details of a Custom Security Policy

Function

This API is used to query the details of a custom security policy.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/security-policies/{security_policy_id}

Table 5-208 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
security_policy_id	Yes	String	Specifies the ID of the custom security policy.

Request Parameters

Table 5-209 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-210 Response body parameters

Parameter	Type	Description
security_policy	**SecurityPolicy** object	This API is used to query the details of a custom security policy.
request_id	String	Specifies the request ID. Note: The value is automatically generated.

Table 5-211 SecurityPolicy

Parameter	Type	Description
id	String	Specifies the ID of the custom security policy.
project_id	String	Specifies the project ID of the custom security policy.
name	String	Specifies the name of the custom security policy.
description	String	Provides supplementary information about the custom security policy.
listeners	Array of **ListenerRef** objects	Specifies the listeners that use the custom security policies.
protocols	Array of strings	Lists the TLS protocols supported by the custom security policy.
ciphers	Array of strings	Lists the cipher suites supported by the custom security policy.
created_at	String	Specifies the time when the custom security policy was created.
updated_at	String	Specifies the time when the custom security policy was updated.

Table 5-212 ListenerRef

Parameter	Type	Description
id	String	Specifies the listener ID.

Example Requests

Querying the details of a custom security policy

```
GET https://{ELB_Endpoint}/v3/7a9941d34fc1497d8d0797429ecfd354/elb/security-policies/
c73e0138-9bdc-40fb-951e-6a1598266ccd
```

Example Responses

Status code: 200

Successful request.

```
{
  "security_policy" : {
    "id" : "c73e0138-9bdc-40fb-951e-6a1598266ccd",
    "name" : "update_securitypolicy",
```



```
    "project_id" : "7a9941d34fc1497d8d0797429ecfd354",
    "description" : "",
    "protocols" : [ "TLSv1", "TLSv1.1", "TLSv1.2", "TLSv1.3" ],
    "ciphers" : [ "AES128-SHA", "AES256-GCM-SHA384", "ECDHE-ECDSA-AES128-GCM-SHA256", "ECDHE-
RSA-AES256-GCM-SHA384", "ECDHE-RSA-AES256-SHA", "TLS_AES_128_GCM_SHA256",
"TLS_AES_256_GCM_SHA384", "TLS_CHACHA20_POLY1305_SHA256", "TLS_AES_128_CCM_SHA256",
"TLS_AES_128_CCM_8_SHA256" ],
    "listeners" : [ {
      "id" : "8e92b7c3-cdae-4039-aa62-c76d09a5950a"
    } ],
    "created_at" : "2021-03-20T09:48:14Z",
    "updated_at" : "2021-03-20T12:45:50Z"
  },
  "request_id" : "dab5d1de-c115-4623-b21d-363478fa0af4"
}
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ShowSecurityPolicySolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowSecurityPolicyRequest request = new ShowSecurityPolicyRequest();
        request.withSecurityPolicyId("{security_policy_id}");
        try {
            ShowSecurityPolicyResponse response = client.showSecurityPolicy(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowSecurityPolicyRequest()
        request.security_policy_id = "{security_policy_id}"
        response = client.show_security_policy(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowSecurityPolicyRequest{}
    request.SecurityPolicyId = "{security_policy_id}"
    response, err := client.ShowSecurityPolicy(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	Successful request.

Error Codes

See **Error Codes**.

5.8.4 Updating a Custom Security Policy

Function

This API is used to update a custom security policy.

Constraints

If **protocols** or **ciphers** is updated, the modification takes effect immediately on all listeners that use the custom security policy. Updating other fields does not affect the listeners.

Calling Method

For details, see **Calling APIs**.

URI

PUT /v3/{project_id}/elb/security-policies/{security_policy_id}

Table 5-213 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
security_policy_id	Yes	String	Specifies the ID of the custom security policy.

Request Parameters

Table 5-214 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Table 5-215 Request body parameters

Parameter	Mandatory	Type	Description
security_policy	Yes	**UpdateSecurityPolicyOption** object	Specifies the custom security policy to be updated.

Table 5-216 UpdateSecurityPolicyOption

Parameter	Mandatory	Type	Description
name	No	String	Specifies the name of the custom security policy.
description	No	String	Provides supplementary information about the custom security policy.
protocols	No	Array of strings	Lists the TLS protocols supported by the custom security policy. Value options: **TLSv1**, **TLSv1.1**, **TLSv1.2**, and **TLSv1.3**

Parameter	Mandatory	Type	Description
ciphers	No	Array of strings	Lists the cipher suites supported by the custom security policy. The following cipher suites are supported: ECDHE-RSA-AES256-GCM-SHA384,ECDHE-RSA-AES128-GCM-SHA256,ECDHE-ECDSA-AES256-GCM-SHA384,ECDHE-ECDSA-AES128-GCM-SHA256,AES128-GCM-SHA256,AES256-GCM-SHA384,ECDHE-ECDSA-AES128-SHA256,ECDHE-RSA-AES128-SHA256,AES128-SHA256,AES256-SHA256,ECDHE-ECDSA-AES256-SHA384,ECDHE-RSA-AES256-SHA384,ECDHE-ECDSA-AES128-SHA,ECDHE-RSA-AES128-SHA,ECDHE-RSA-AES256-SHA,ECDHE-ECDSA-AES256-SHA,AES128-SHA,AES256-SHA,CAMELLIA128-SHA,DES-CBC3-SHA,CAMELLIA256-SHA,ECDHE-RSA-CHACHA20-POLY1305,ECDHE-ECDSA-CHACHA20-POLY1305,TLS_AES_128_GCM_SHA256,TLS_AES_256_GCM_SHA384,TLS_CHACHA20_POLY1305_SHA256,TLS_AES_128_CCM_SHA256,TLS_AES_128_CCM_8_SHA256 Note: • The protocol and cipher suite must match. At least one cipher suite must match the protocol. • You can match the protocol and cipher suite based on system security policy.

Response Parameters

Status code: 200

Table 5-217 Response body parameters

Parameter	Type	Description
security_policy	**SecurityPolicy** object	Specifies the custom security policy that has been updated.
request_id	String	Specifies the request ID. Note: The value is automatically generated.

Table 5-218 SecurityPolicy

Parameter	Type	Description
id	String	Specifies the ID of the custom security policy.
project_id	String	Specifies the project ID of the custom security policy.
name	String	Specifies the name of the custom security policy.
description	String	Provides supplementary information about the custom security policy.
listeners	Array of **ListenerRef** objects	Specifies the listeners that use the custom security policies.
protocols	Array of strings	Lists the TLS protocols supported by the custom security policy.
ciphers	Array of strings	Lists the cipher suites supported by the custom security policy.
created_at	String	Specifies the time when the custom security policy was created.
updated_at	String	Specifies the time when the custom security policy was updated.

Table 5-219 ListenerRef

Parameter	Type	Description
id	String	Specifies the listener ID.

Example Requests

Changing the TLS protocol and cipher suite used by a custom security policy


```
PUT https://{ELB_Endpoint}/v3/7a9941d34fc1497d8d0797429ecfd354/elb/security-policies/
c73e0138-9bdc-40fb-951e-6a1598266ccd

{
  "security_policy" : {
    "name" : "update_securitypolicy",
    "protocols" : [ "TLSv1.2", "TLSv1.1", "TLSv1.3" ],
    "ciphers" : [ "CAMELLIA128-SHA", "TLS_CHACHA20_POLY1305_SHA256", "TLS_AES_128_CCM_SHA256",
"TLS_AES_128_CCM_8_SHA256" ]
  }
}
```

Example Responses

Status code: 200

Successful request.

```
{
  "request_id" : "7fa73388-06b7-476d-9b0b-64f83de86ed4",
  "security_policy" : {
    "id" : "c73e0138-9bdc-40fb-951e-6a1598266ccd",
    "name" : "update_securitypolicy",
    "project_id" : "7a9941d34fc1497d8d0797429ecfd354",
    "description" : "",
    "protocols" : [ "TLSv1.2", "TLSv1.1", "TLSv1.3" ],
    "ciphers" : [ "CAMELLIA128-SHA", "TLS_CHACHA20_POLY1305_SHA256", "TLS_AES_128_CCM_SHA256",
"TLS_AES_128_CCM_8_SHA256" ],
    "listeners" : [ {
      "id" : "8e92b7c3-cdae-4039-aa62-c76d09a5950a"
    } ],
    "created_at" : "2021-03-20T09:48:14Z",
    "updated_at" : "2021-03-26T01:30:31Z"
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Changing the TLS protocol and cipher suite used by a custom security policy

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;

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

public class UpdateSecurityPolicySolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdateSecurityPolicyRequest request = new UpdateSecurityPolicyRequest();
        request.withSecurityPolicyId("{security_policy_id}");
        UpdateSecurityPolicyRequestBody body = new UpdateSecurityPolicyRequestBody();
        List<UpdateSecurityPolicyOption.CiphersEnum> listSecurityPolicyCiphers = new ArrayList<>();
        listSecurityPolicyCiphers.add(UpdateSecurityPolicyOption.CiphersEnum.fromValue("CAMELLIA128-
SHA"));

listSecurityPolicyCiphers.add(UpdateSecurityPolicyOption.CiphersEnum.fromValue("TLS_CHACHA20_POLY13
05_SHA256"));

listSecurityPolicyCiphers.add(UpdateSecurityPolicyOption.CiphersEnum.fromValue("TLS_AES_128_CCM_SHA2
56"));

listSecurityPolicyCiphers.add(UpdateSecurityPolicyOption.CiphersEnum.fromValue("TLS_AES_128_CCM_8_SH
A256"));
        List<String> listSecurityPolicyProtocols = new ArrayList<>();
        listSecurityPolicyProtocols.add("TLSv1.2");
        listSecurityPolicyProtocols.add("TLSv1.1");
        listSecurityPolicyProtocols.add("TLSv1.3");
        UpdateSecurityPolicyOption securityPolicybody = new UpdateSecurityPolicyOption();
        securityPolicybody.withName("update_securitypolicy")
            .withProtocols(listSecurityPolicyProtocols)
            .withCiphers(listSecurityPolicyCiphers);
        body.withSecurityPolicy(securityPolicybody);
        request.withBody(body);
        try {
            UpdateSecurityPolicyResponse response = client.updateSecurityPolicy(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

Changing the TLS protocol and cipher suite used by a custom security policy

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdateSecurityPolicyRequest()
        request.security_policy_id = "{security_policy_id}"
        listCiphersSecurityPolicy = [
            "CAMELLIA128-SHA",
            "TLS_CHACHA20_POLY1305_SHA256",
            "TLS_AES_128_CCM_SHA256",
            "TLS_AES_128_CCM_8_SHA256"
        ]
        listProtocolsSecurityPolicy = [
            "TLSv1.2",
            "TLSv1.1",
            "TLSv1.3"
        ]
        securityPolicybody = UpdateSecurityPolicyOption(
            name="update_securitypolicy",
            protocols=listProtocolsSecurityPolicy,
            ciphers=listCiphersSecurityPolicy
        )
        request.body = UpdateSecurityPolicyRequestBody(
            security_policy=securityPolicybody
        )
        response = client.update_security_policy(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

Changing the TLS protocol and cipher suite used by a custom security policy

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdateSecurityPolicyRequest{}
    request.SecurityPolicyId = "{security_policy_id}"
    var listCiphersSecurityPolicy = []model.UpdateSecurityPolicyOptionCiphers{
        model.GetUpdateSecurityPolicyOptionCiphersEnum().CAMELLIA128_SHA,
        model.GetUpdateSecurityPolicyOptionCiphersEnum().TLS_CHACHA20_POLY1305_SHA256,
        model.GetUpdateSecurityPolicyOptionCiphersEnum().TLS_AES_128_CCM_SHA256,
        model.GetUpdateSecurityPolicyOptionCiphersEnum().TLS_AES_128_CCM_8_SHA256,
    }
    var listProtocolsSecurityPolicy = []string{
        "TLSv1.2",
        "TLSv1.1",
        "TLSv1.3",
    }
    nameSecurityPolicy:= "update_securitypolicy"
    securityPolicybody := &model.UpdateSecurityPolicyOption{
        Name: &nameSecurityPolicy,
        Protocols: &listProtocolsSecurityPolicy,
        Ciphers: &listCiphersSecurityPolicy,
    }
    request.Body = &model.UpdateSecurityPolicyRequestBody{
        SecurityPolicy: securityPolicybody,
    }
    response, err := client.UpdateSecurityPolicy(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	Successful request.

Error Codes

See **Error Codes**.

5.8.5 Deleting a Custom Security Policy

Function

This API is used to delete a custom security policy.

Constraints

A custom security policy that has been used by a listener cannot be deleted.

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v3/{project_id}/elb/security-policies/{security_policy_id}

Table 5-220 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
security_policy_id	Yes	String	Specifies the ID of the custom security policy.

Request Parameters

Table 5-221 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

None

Example Requests

Deleting a custom security policy

```
DELETE https://{ELB_Endpoint}/v3/45977fa2dbd7482098dd68d0d8970117/elb/security-policies/8722e0e0-9cc9-4490-9660-8c9a5732fbb0
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class DeleteSecurityPolicySolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteSecurityPolicyRequest request = new DeleteSecurityPolicyRequest();
        request.withSecurityPolicyId("{security_policy_id}");
        try {
            DeleteSecurityPolicyResponse response = client.deleteSecurityPolicy(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteSecurityPolicyRequest()
        request.security_policy_id = "{security_policy_id}"
        response = client.delete_security_policy(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteSecurityPolicyRequest{}
    request.SecurityPolicyId = "{security_policy_id}"
    response, err := client.DeleteSecurityPolicy(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	Successful request.

Error Codes

See **Error Codes**.

5.8.6 Querying System Security Policies

Function

This API is used to query system security policies.

System security policies are available to all users and cannot be created or modified.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/system-security-policies

Table 5-222 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Request Parameters

Table 5-223 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-224 Response body parameters

Parameter	Type	Description
system_security_policies	Array of **SystemSecurityPolicy** objects	Lists system security policies.
request_id	String	Specifies the request ID. Note: The value is automatically generated.

Table 5-225 SystemSecurityPolicy

Parameter	Type	Description
name	String	Specifies the name of the system security policy.
protocols	String	Lists the TLS protocols supported by the system security policy.
ciphers	String	Lists the cipher suites supported by the system security policy.
project_id	String	Specifies the project ID.

Example Requests

Querying system security policies

```
GET https://{ELB_Endpoint}/v3/7a9941d34fc1497d8d0797429ecfd354/elb/system-security-policies
```

Example Responses

Status code: 200

Successful request.


```
{
  "request_id" : "fa83d976-e617-4a96-9a43-5bdb33011f30",
  "system_security_policies" : [ {
    "name" : "tls-1-0",
    "project_id" : "7a9941d34fc1497d8d0797429ecfd354",
    "protocols" : "TLSv1.2 TLSv1.1 TLSv1",
    "ciphers" : "ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES128-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-ECDSA-AES256-
SHA:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-
GCM-SHA384:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-RSA-AES256-
SHA384:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:AES128-SHA:AES256-SHA"
  }, {
    "name" : "tls-1-0-inherit",
    "project_id" : "7a9941d34fc1497d8d0797429ecfd354",
    "protocols" : "TLSv1.2 TLSv1.1 TLSv1",
    "ciphers" : "ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES128-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-ECDSA-AES256-
SHA:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-
GCM-SHA384:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-RSA-AES256-
SHA384:ECDHE-RSA-AES128-SHA:DHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:AES128-SHA:AES256-
SHA:DHE-DSS-AES128-SHA:CAMELLIA128-SHA:EDH-RSA-DES-CBC3-SHA:DES-CBC3-SHA:ECDHE-RSA-RC4-
SHA:RC4-SHA:DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:DHE-RSA-CAMELLIA256-SHA:DHE-DSS-
CAMELLIA256-SHA:CAMELLIA256-SHA:EDH-DSS-DES-CBC3-SHA:DHE-RSA-CAMELLIA128-SHA:DHE-DSS-
CAMELLIA128-SHA"
  }, {
    "name" : "tls-1-1",
    "project_id" : "7a9941d34fc1497d8d0797429ecfd354",
    "protocols" : "TLSv1.2 TLSv1.1",
    "ciphers" : "ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES128-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-ECDSA-AES256-
SHA:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-
GCM-SHA384:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-RSA-AES256-
SHA384:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:AES128-SHA:AES256-SHA"
  }, {
    "name" : "tls-1-2",
    "project_id" : "7a9941d34fc1497d8d0797429ecfd354",
    "protocols" : "TLSv1.2",
    "ciphers" : "ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES128-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-ECDSA-AES256-
SHA:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-
GCM-SHA384:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-RSA-AES256-
SHA384:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:AES128-SHA:AES256-SHA"
  }, {
    "name" : "tls-1-2-strict",
    "project_id" : "7a9941d34fc1497d8d0797429ecfd354",
    "protocols" : "TLSv1.2",
    "ciphers" : "ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES128-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-
GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-RSA-AES128-SHA256:AES128-
SHA256:AES256-SHA256:ECDHE-RSA-AES256-SHA384"
  }, {
    "name" : "tls-1-2-fs",
    "project_id" : "7a9941d34fc1497d8d0797429ecfd354",
    "protocols" : "TLSv1.2",
    "ciphers" : "ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES128-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-
GCM-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384"
  }, {
    "name" : "tls-1-0-with-1-3",
    "project_id" : "7a9941d34fc1497d8d0797429ecfd354",
    "protocols" : "TLSv1.3 TLSv1.2 TLSv1.1 TLSv1",
    "ciphers" : "ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES128-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-ECDSA-AES256-
SHA:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-
GCM-SHA384:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-RSA-AES256-
SHA384:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:AES128-SHA:AES256-
SHA:TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_1
28_CCM_SHA256:TLS_AES_128_CCM_8_SHA256"
```



```
  }, {
    "name" : "tls-1-2-fs-with-1-3",
    "project_id" : "7a9941d34fc1497d8d0797429ecfd354",
    "protocols" : "TLSv1.3 TLSv1.2",
    "ciphers" : "ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES128-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-
GCM-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-
SHA384:TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_A
ES_128_CCM_SHA256:TLS_AES_128_CCM_8_SHA256"
  }, {
    "name" : "hybrid-policy-1-0",
    "project_id" : "7a9941d34fc1497d8d0797429ecfd354",
    "protocols" : "TLSv1.2 TLSv1.1",
    "ciphers" : "ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES128-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-ECDSA-AES256-
SHA:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-
GCM-SHA384:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-RSA-AES256-
SHA384:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:AES128-SHA:AES256-SHA"
  }, {
    "name" : "tls-1-2-strict-no-cbc",
    "project_id" : "7a9941d34fc1497d8d0797429ecfd354",
    "protocols" : "TLSv1.2",
    "ciphers" : "ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-
AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256"
  } ]
}
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ListSystemSecurityPoliciesSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ListSystemSecurityPoliciesRequest request = new ListSystemSecurityPoliciesRequest();
        try {
```

```
            ListSystemSecurityPoliciesResponse response = client.listSystemSecurityPolicies(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListSystemSecurityPoliciesRequest()
        response = client.list_system_security_policies(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListSystemSecurityPoliciesRequest{}
    response, err := client.ListSystemSecurityPolicies(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	Successful request.

Error Codes

See **Error Codes**.

5.9 IP Address Group

5.9.1 Creating an IP Address Group

Function

This API is used to create an IP address group.

Each IP address group can contain a single IP address, IP address ranges, or CIDR blocks. Each IP address range must be in the format of *ip-ip*, for example, 10.12.3.1-10.12.3.10. Both IPv4 and IPv6 addresses are supported.

0.0.0.0 will be considered the same as 0.0.0.0/32. If you enter both 0.0.0.0 and 0.0.0.0/32, only one will be kept. 0:0:0:0:0:0:0:1 will be considered the same as ::1 and ::1/128. If you enter 0:0:0:0:0:0:0:1, ::1 and ::1/128, only one will be kept.

Calling Method

For details, see **Calling APIs**.

URI

POST /v3/{project_id}/elb/ipgroups

Table 5-226 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Request Parameters

Table 5-227 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Table 5-228 Request body parameters

Parameter	Mandatory	Type	Description
ipgroup	Yes	**CreateIpGroupOption** object	Specifies the request body for creating an IP address group.

Table 5-229 CreateIpGroupOption

Parameter	Mandatory	Type	Description
project_id	No	String	Specifies the project ID of the IP address group.
description	No	String	Provides supplementary information about the IP address group.
name	No	String	Specifies the IP address group name.

Parameter	Mandatory	Type	Description
ip_list	Yes	Array of **CreateIpGroupIpOption** objects	Specifies the IP addresses or CIDR blocks in the IP address group. **[]** indicates any IP address.
enterprise_project_id	No	String	Specifies the ID of the enterprise project that the IP address group belongs to.

Table 5-230 CreateIpGroupIpOption

Parameter	Mandatory	Type	Description
ip	Yes	String	Specifies the IP addresses in the IP address group. An IP address range can be in the format of *ip-ip*, for example, 192.168.1.2-192.168.2.253 or 2001:0DB8:02de::0e12-2001:0DB8:02de::0e13. The end IP address must be greater than the start IP address.
description	No	String	Provides remarks about the IP address group.

Response Parameters

Status code: 201

Table 5-231 Response body parameters

Parameter	Type	Description
ipgroup	**IpGroup** object	Specifies the response body for creating an IP address group.
request_id	String	Specifies the request ID. Note: The value is automatically generated.

Table 5-232 IpGroup

Parameter	Type	Description
id	String	Specifies the ID of the IP address group.
name	String	Specifies the IP address group name.
description	String	Provides supplementary information about the IP address group.
ip_list	Array of **IpInfo** objects	Specifies the IP addresses or CIDR blocks in the IP address group. **[]** indicates any IP address.
listeners	Array of **ListenerRef** objects	Lists the IDs of listeners with which the IP address group is associated.
project_id	String	Specifies the project ID of the IP address group.
enterprise_project_id	String	Specifies the ID of the enterprise project that the IP address group belongs to.
created_at	String	Specifies the time when the IP address group was created.
updated_at	String	Specifies the time when the IP address group was updated.

Table 5-233 IpInfo

Parameter	Type	Description
ip	String	Specifies the IP addresses in the IP address group.
description	String	Provides remarks about the IP address group.

Table 5-234 ListenerRef

Parameter	Type	Description
id	String	Specifies the listener ID.

Example Requests

Creating an IP address group and specifying IP addresses


```
POST https://{ELB_Endpoint}/v3/45977fa2dbd7482098dd68d0d8970117/elb/ipgroups

{
  "ipgroup" : {
    "name" : "test_ipg",
    "ip_list" : [ {
      "ip" : "192.168.1.123"
    }, {
      "ip" : "192.168.3.0/24",
      "description" : "test_ip"
    }, {
      "ip" : "2001:0DB8:02de:0000:0000:0000:0000:0e13"
    } ]
  }
}
```

Example Responses

Status code: 201

Normal response to POST requests.

```
{
  "ipgroup" : {
    "description" : "",
    "id" : "8722e0e0-9cc9-4490-9660-8c9a5732fbb0",
    "name" : "test_ipg",
    "project_id" : "45977fa2dbd7482098dd68d0d8970117",
    "ip_list" : [ {
      "ip" : "192.168.1.123",
      "description" : ""
    }, {
      "ip" : "192.168.3.0/24",
      "description" : "test_ip"
    } ],
    "listeners" : [ {
      "id" : "88f9c079-29cb-435a-b98f-0c5c0b90c2bd"
    }, {
      "id" : "2f4c9644-d5d2-4cf8-a3c0-944239a4f58c"
    } ],
    "created_at" : "2018-01-16T03:19:16",
    "updated_at" : "2018-01-16T03:19:16"
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Creating an IP address group and specifying IP addresses

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;

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



```
public class CreateIpGroupSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateIpGroupRequest request = new CreateIpGroupRequest();
        CreateIpGroupRequestBody body = new CreateIpGroupRequestBody();
        List<CreateIpGroupIpOption> listIpgroupIpList = new ArrayList<>();
        listIpgroupIpList.add(
            new CreateIpGroupIpOption()
                .withIp("192.168.1.123")
        );
        listIpgroupIpList.add(
            new CreateIpGroupIpOption()
                .withIp("192.168.3.0/24")
                .withDescription("test_ip")
        );
        listIpgroupIpList.add(
            new CreateIpGroupIpOption()
                .withIp("2001:0DB8:02de:0000:0000:0000:0000:0e13")
        );
        CreateIpGroupOption ipgroupbody = new CreateIpGroupOption();
        ipgroupbody.withName("test_ipg")
            .withIpList(listIpgroupIpList);
        body.withIpgroup(ipgroupbody);
        request.withBody(body);
        try {
            CreateIpGroupResponse response = client.createIpGroup(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

Creating an IP address group and specifying IP addresses

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
```

```
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateIpGroupRequest()
        listIpListIpgroup = [
            CreateIpGroupIpOption(
                ip="192.168.1.123"
            ),
            CreateIpGroupIpOption(
                ip="192.168.3.0/24",
                description="test_ip"
            ),
            CreateIpGroupIpOption(
                ip="2001:0DB8:02de:0000:0000:0000:0000:0e13"
            )
        ]
        ipgroupbody = CreateIpGroupOption(
            name="test_ipg",
            ip_list=listIpListIpgroup
        )
        request.body = CreateIpGroupRequestBody(
            ipgroup=ipgroupbody
        )
        response = client.create_ip_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

Creating an IP address group and specifying IP addresses

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateIpGroupRequest{}
    descriptionIpList:= "test_ip"
    var listIpListIpgroup = []model.CreateIpGroupIpOption{
        {
            Ip: "192.168.1.123",
        },
        {
            Ip: "192.168.3.0/24",
            Description: &descriptionIpList,
        },
        {
            Ip: "2001:0DB8:02de:0000:0000:0000:0000:0e13",
        },
    }
    nameIpgroup:= "test_ipg"
    ipgroupbody := &model.CreateIpGroupOption{
        Name: &nameIpgroup,
        IpList: listIpListIpgroup,
    }
    request.Body = &model.CreateIpGroupRequestBody{
        Ipgroup: ipgroupbody,
    }
    response, err := client.CreateIpGroup(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 POST requests.

Error Codes

See **Error Codes**.

5.9.2 Querying IP Address Groups

Function

This API is used to query IP address groups.

Constraints

This API has the following constraints:

- Parameters **marker**, **limit**, and **page_reverse** are used for pagination query.
- Parameters **marker** and **page_reverse** take effect only when they are used together with parameter **limit**.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/ipgroups

Table 5-235 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Table 5-236 Query Parameters

Parameter	Mandatory	Type	Description
marker	No	String	Specifies the ID of the last record on the previous page. Note: • This parameter must be used together with **limit**. • If this parameter is not specified, the first page will be queried. • This parameter cannot be left blank or set to an invalid ID.
limit	No	Integer	Specifies the number of records on each page. Value range: 0–2000 Default value: 2000

Parameter	Mandatory	Type	Description
page_reverse	No	Boolean	Specifies whether to use reverse query. Value options: • **true**: Query the previous page. • **false** (default): Query the next page. Note: • This parameter must be used together with **limit**. • If **page_reverse** is set to **true** and you want to query the previous page, set the value of **marker** to the value of **previous_marker**.
id	No	Array of strings	Specifies the ID of the IP address group.
name	No	Array of strings	Specifies the name of the IP address group.
description	No	Array of strings	Provides supplementary information about the IP address group.
ip_list	No	Array of strings	Lists the IP addresses in the IP address group. Multiple IP addresses are separated with commas.

Parameter	Mandatory	Type	Description
enterprise_project_id	No	Array of strings	Specifies the ID of the enterprise project. • If **enterprise_project_id** is not specified, resources in all enterprise projects are queried by default. Fine-grained authorization is performed. The **elb:ipgroups:list** permission must be assigned to the user group. • If **enterprise_project_id** is specified, the value can be a specific enterprise project ID or **all_granted_eps**. If the value is a specific enterprise project ID, only resources in the enterprise project are queried. If the value is **all_granted_eps**, resources in the enterprise projects with the **elb:ipgroups:list** permission are queried. Multiple values can be queried in the format of *enterprise_project_id=xxx&enterprise_project_id=xxx*.

Request Parameters

Table 5-237 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-238 Response body parameters

Parameter	Type	Description
ipgroups	Array of **IpGroup** objects	Lists the returned IP address groups.
request_id	String	Specifies the request ID. Note: The value is automatically generated.
page_info	**PageInfo** object	Shows pagination information.

Table 5-239 IpGroup

Parameter	Type	Description
id	String	Specifies the ID of the IP address group.
name	String	Specifies the IP address group name.
description	String	Provides supplementary information about the IP address group.
ip_list	Array of **IpInfo** objects	Specifies the IP addresses or CIDR blocks in the IP address group. **[]** indicates any IP address.
listeners	Array of **ListenerRef** objects	Lists the IDs of listeners with which the IP address group is associated.
project_id	String	Specifies the project ID of the IP address group.
enterprise_project_id	String	Specifies the ID of the enterprise project that the IP address group belongs to.
created_at	String	Specifies the time when the IP address group was created.
updated_at	String	Specifies the time when the IP address group was updated.

Table 5-240 IpInfo

Parameter	Type	Description
ip	String	Specifies the IP addresses in the IP address group.

Parameter	Type	Description
description	String	Provides remarks about the IP address group.

Table 5-241 ListenerRef

Parameter	Type	Description
id	String	Specifies the listener ID.

Table 5-242 PageInfo

Parameter	Type	Description
previous_marker	String	Specifies the ID of the first record in the pagination query result. When **page_reverse** is set to **true**, this parameter is used together to query resources on the previous page.
next_marker	String	Specifies the ID of the last record in the pagination query result.
current_count	Integer	Specifies the number of records.

Example Requests

Querying IP address groups on each page

```
GET https://{ELB_Endpoint}/v3/45977fa2dbd7482098dd68d0d8970117/elb/ipgroups?limit=1
```

Example Responses

Status code: 200

Successful request.

```
{
  "ipgroups" : [ {
    "description" : "",
    "id" : "8722e0e0-9cc9-4490-9660-8c9a5732fbb0",
    "name" : "test_ipg",
    "project_id" : "45977fa2dbd7482098dd68d0d8970117",
    "ip_list" : [ {
      "ip" : "192.168.1.123",
      "description" : ""
    }, {
      "ip" : "192.168.3.0/24",
      "description" : "test_ip"
    } ],
    "listeners" : [ {
      "id" : "88f9c079-29cb-435a-b98f-0c5c0b90c2bd"
    }, {
```



```
      "id" : "2f4c9644-d5d2-4cf8-a3c0-944239a4f58c"
    } ],
    "created_at" : "2018-01-16T03:19:16",
    "updated_at" : "2018-01-16T03:19:16"
  } ],
  "page_info" : {
    "previous_marker" : "1d321f77-bc7b-45d3-9cfe-d7c0b65a3620",
    "current_count" : 1
  },
  "request_id" : "8d9f423c-8766-4b6a-9952-275a88ac1ce3"
}
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ListIpGroupsSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ListIpGroupsRequest request = new ListIpGroupsRequest();
        try {
            ListIpGroupsResponse response = client.listIpGroups(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListIpGroupsRequest()
        response = client.list_ip_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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
```



```
        Build())

    request := &model.ListIpGroupsRequest{}
    response, err := client.ListIpGroups(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	Successful request.

Error Codes

See **Error Codes**.

5.9.3 Querying the Details of an IP Address Group

Function

This API is used to view the details of an IP address group.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/ipgroups/{ipgroup_id}

Table 5-243 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
ipgroup_id	Yes	String	Specifies the ID of the IP address group.

Request Parameters

Table 5-244 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-245 Response body parameters

Parameter	Type	Description
ipgroup	**IpGroup** object	Specifies the response body for querying the details of the IP address group.
request_id	String	Specifies the request ID. Note: The value is automatically generated.

Table 5-246 IpGroup

Parameter	Type	Description
id	String	Specifies the ID of the IP address group.
name	String	Specifies the IP address group name.
description	String	Provides supplementary information about the IP address group.
ip_list	Array of **IpInfo** objects	Specifies the IP addresses or CIDR blocks in the IP address group. **[]** indicates any IP address.
listeners	Array of **ListenerRef** objects	Lists the IDs of listeners with which the IP address group is associated.
project_id	String	Specifies the project ID of the IP address group.
enterprise_project_id	String	Specifies the ID of the enterprise project that the IP address group belongs to.

Parameter	Type	Description
created_at	String	Specifies the time when the IP address group was created.
updated_at	String	Specifies the time when the IP address group was updated.

Table 5-247 IpInfo

Parameter	Type	Description
ip	String	Specifies the IP addresses in the IP address group.
description	String	Provides remarks about the IP address group.

Table 5-248 ListenerRef

Parameter	Type	Description
id	String	Specifies the listener ID.

Example Requests

Querying the details of an IP address group

```
GET https://{ELB_Endpoint}/v3/45977fa2dbd7482098dd68d0d8970117/elb/ipgroups/
8722e0e0-9cc9-4490-9660-8c9a5732fbb0
```

Example Responses

Status code: 200

Successful request.

```
{
  "ipgroup" : {
    "description" : "",
    "id" : "8722e0e0-9cc9-4490-9660-8c9a5732fbb0",
    "name" : "test_ipg",
    "project_id" : "45977fa2dbd7482098dd68d0d8970117",
    "ip_list" : [ {
      "ip" : "192.168.1.123",
      "description" : ""
    }, {
      "ip" : "192.168.3.0/24",
      "description" : "test_ip"
    } ],
    "listeners" : [ {
      "id" : "88f9c079-29cb-435a-b98f-0c5c0b90c2bd"
    }, {
      "id" : "2f4c9644-d5d2-4cf8-a3c0-944239a4f58c"
```



```
    } ],
    "created_at" : "2018-01-16T03:19:16",
    "updated_at" : "2018-01-16T03:19:16"
  }
}
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ShowIpGroupSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowIpGroupRequest request = new ShowIpGroupRequest();
        request.withIpgroupId("{ipgroup_id}");
        try {
            ShowIpGroupResponse response = client.showIpGroup(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowIpGroupRequest()
        request.ipgroup_id = "{ipgroup_id}"
        response = client.show_ip_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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowIpGroupRequest{}
```



```
    request.IpgroupId = "{ipgroup_id}"
    response, err := client.ShowIpGroup(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	Successful request.

Error Codes

See **Error Codes**.

5.9.4 Updating an IP Address Group

Function

This API is used to update an IP address group.

All IP addresses in the IP address group will be overwritten, and the IP addresses that are not included in the **ip_list** parameter in the request body will be removed.

Each IP address group can contain a single IP address, IP address ranges, or CIDR blocks. Each IP address range must be in the format of *ip-ip*, for example, 10.12.3.1-10.12.3.10. Both IPv4 and IPv6 addresses are supported.

0.0.0.0 will be considered the same as 0.0.0.0/32. If you enter both 0.0.0.0 and 0.0.0.0/32, only one will be kept. 0:0:0:0:0:0:0:1 will be considered the same as ::1 and ::1/128. If you enter 0:0:0:0:0:0:0:1, ::1 and ::1/128, only one will be kept.

Calling Method

For details, see **Calling APIs**.

URI

PUT /v3/{project_id}/elb/ipgroups/{ipgroup_id}

Table 5-249 Path Parameters

Parameter	Mandatory	Type	Description
ipgroup_id	Yes	String	Specifies the ID of the IP address group.
project_id	Yes	String	Specifies the project ID.

Request Parameters

Table 5-250 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Table 5-251 Request body parameters

Parameter	Mandatory	Type	Description
ipgroup	Yes	**UpdateIpGroupOption** object	Specifies the request body for updating the IP address group.

Table 5-252 UpdateIpGroupOption

Parameter	Mandatory	Type	Description
description	No	String	Provides supplementary information about the IP address group.
name	No	String	Specifies the IP address group name.
ip_list	No	Array of **UpadateIpGroupIpOption** objects	Lists the IP addresses in the IP address group.

Table 5-253 UpadateIpGroupIpOption

Parameter	Mandatory	Type	Description
ip	Yes	String	Specifies the IP addresses or IP address ranges in the IP address group. IPv4 and IPv6 addresses are supported. An IP address range can be in the format of *ip-ip*, for example, 192.168.1.2-192.168.2.253 or 2001:0DB8:02de::0e12-2001:0DB8:02de::0e13. The end IP address must be greater than the start IP address. Specified IP addresses that are not already in the IP address group will be added; existing ones will have their descriptions updated.
description	No	String	Provides remarks about the IP address group.

Response Parameters

Status code: 200

Table 5-254 Response body parameters

Parameter	Type	Description
ipgroup	**IpGroup** object	Specifies the response body for updating the IP address group.
request_id	String	Specifies the request ID. Note: The value is automatically generated.

Table 5-255 IpGroup

Parameter	Type	Description
id	String	Specifies the ID of the IP address group.
name	String	Specifies the IP address group name.
description	String	Provides supplementary information about the IP address group.

Parameter	Type	Description
ip_list	Array of **IpInfo** objects	Specifies the IP addresses or CIDR blocks in the IP address group. **[]** indicates any IP address.
listeners	Array of **ListenerRef** objects	Lists the IDs of listeners with which the IP address group is associated.
project_id	String	Specifies the project ID of the IP address group.
enterprise_project_id	String	Specifies the ID of the enterprise project that the IP address group belongs to.
created_at	String	Specifies the time when the IP address group was created.
updated_at	String	Specifies the time when the IP address group was updated.

Table 5-256 IpInfo

Parameter	Type	Description
ip	String	Specifies the IP addresses in the IP address group.
description	String	Provides remarks about the IP address group.

Table 5-257 ListenerRef

Parameter	Type	Description
id	String	Specifies the listener ID.

Example Requests

Changing all the IP addresses in an IP address group

```
PUT https://{ELB_Endpoint}/v3/45977fa2dbd7482098dd68d0d8970117/elb/ipgroups/
8722e0e0-9cc9-4490-9660-8c9a5732fbb0

{
  "ipgroup" : {
    "name" : "test_ipg",
    "ip_list" : [ {
      "ip" : "192.168.1.123"
    }, {
      "ip" : "192.168.3.0/24",
```



```
    "description" : "test_ip"
  } ]
 }
}
```

Example Responses

Status code: 200

Successful request.

```
{
 "ipgroup" : {
  "description" : "",
  "id" : "8722e0e0-9cc9-4490-9660-8c9a5732fbb0",
  "name" : "test_ipg",
  "project_id" : "45977fa2dbd7482098dd68d0d8970117",
  "ip_list" : [ {
   "ip" : "192.168.1.123",
   "description" : ""
  }, {
   "ip" : "192.168.3.0/24",
   "description" : "test_ip"
  } ],
  "listeners" : [ {
   "id" : "88f9c079-29cb-435a-b98f-0c5c0b90c2bd"
  }, {
   "id" : "2f4c9644-d5d2-4cf8-a3c0-944239a4f58c"
  } ],
  "created_at" : "2018-01-16T03:19:16",
  "updated_at" : "2018-01-16T03:19:16"
 }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Changing all the IP addresses in an IP address group

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;

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

public class UpdateIpGroupSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdateIpGroupRequest request = new UpdateIpGroupRequest();
        request.withIpgroupId("{ipgroup_id}");
        UpdateIpGroupRequestBody body = new UpdateIpGroupRequestBody();
        List<UpadateIpGroupIpOption> listIpgroupIpList = new ArrayList<>();
        listIpgroupIpList.add(
            new UpadateIpGroupIpOption()
                .withIp("192.168.1.123")
        );
        listIpgroupIpList.add(
            new UpadateIpGroupIpOption()
                .withIp("192.168.3.0/24")
                .withDescription("test_ip")
        );
        UpdateIpGroupOption ipgroupbody = new UpdateIpGroupOption();
        ipgroupbody.withName("test_ipg")
            .withIpList(listIpgroupIpList);
        body.withIpgroup(ipgroupbody);
        request.withBody(body);
        try {
            UpdateIpGroupResponse response = client.updateIpGroup(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

Changing all the IP addresses in an IP address group

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdateIpGroupRequest()
        request.ipgroup_id = "{ipgroup_id}"
        listIpListIpgroup = [
            UpadateIpGroupIpOption(
                ip="192.168.1.123"
            ),
            UpadateIpGroupIpOption(
                ip="192.168.3.0/24",
                description="test_ip"
            )
        ]
        ipgroupbody = UpdateIpGroupOption(
            name="test_ipg",
            ip_list=listIpListIpgroup
        )
        request.body = UpdateIpGroupRequestBody(
            ipgroup=ipgroupbody
        )
        response = client.update_ip_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

Changing all the IP addresses in an IP address group

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())
```



```
    request := &model.UpdateIpGroupRequest{}
    request.IpgroupId = "{ipgroup_id}"
    descriptionIpList:= "test_ip"
    var listIpListIpgroup = []model.UpadateIpGroupIpOption{
        {
            Ip: "192.168.1.123",
        },
        {
            Ip: "192.168.3.0/24",
            Description: &descriptionIpList,
        },
    }
    nameIpgroup:= "test_ipg"
    ipgroupbody := &model.UpdateIpGroupOption{
        Name: &nameIpgroup,
        IpList: &listIpListIpgroup,
    }
    request.Body = &model.UpdateIpGroupRequestBody{
        Ipgroup: ipgroupbody,
    }
    response, err := client.UpdateIpGroup(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	Successful request.

Error Codes

See **Error Codes**.

5.9.5 Deleting an IP Address Group

Function

This API is used to delete an IP address group.

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v3/{project_id}/elb/ipgroups/{ipgroup_id}

Table 5-258 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
ipgroup_id	Yes	String	Specifies the ID of the IP address group.

Request Parameters

Table 5-259 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

None

Example Requests

Deleting an IP address group

```
DELETE https://{ELB_Endpoint}/v3/45977fa2dbd7482098dd68d0d8970117/elb/ipgroups/
8722e0e0-9cc9-4490-9660-8c9a5732fbb0
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class DeleteIpGroupSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteIpGroupRequest request = new DeleteIpGroupRequest();
        request.withIpgroupId("{ipgroup_id}");
        try {
            DeleteIpGroupResponse response = client.deleteIpGroup(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteIpGroupRequest()
        request.ipgroup_id = "{ipgroup_id}"
        response = client.delete_ip_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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteIpGroupRequest{}
    request.IpgroupId = "{ipgroup_id}"
    response, err := client.DeleteIpGroup(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	Successful request.

Error Codes

See **Error Codes**.

5.9.6 Updating IP Addresses in an IP Address Group

Function

This API is used to update the IP addresses in an IP address group.

Calling Method

For details, see **Calling APIs**.

URI

POST /v3/{project_id}/elb/ipgroups/{ipgroup_id}/iplist/create-or-update

Table 5-260 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
ipgroup_id	Yes	String	Specifies the ID of the IP address group.

Request Parameters

Table 5-261 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	Specifies the token used for IAM authentication.

Table 5-262 Request body parameters

Parameter	Mandatory	Type	Description
ipgroup	No	**UpdateIpList Option** object	Specifies the request parameter for updating the IP addresses of an IP address group.

Table 5-263 UpdateIpListOption

Parameter	Mandatory	Type	Description
name	No	String	Specifies the name of the IP address group.
ip_list	No	Array of **UpadateIpGroupIpOption** objects	Specifies the IP addresses in the IP address group.
description	No	String	Specifies supplementary information about the IP address group.

Table 5-264 UpadateIpGroupIpOption

Parameter	Mandatory	Type	Description
ip	Yes	String	Specifies the IP addresses or IP address ranges in the IP address group. IPv4 and IPv6 addresses are supported. An IP address range can be in the format of *ip-ip*, for example, 192.168.1.2-192.168.2.253 or 2001:0DB8:02de::0e12-2001:0DB8:02de::0e13. The end IP address must be greater than the start IP address. Specified IP addresses that are not already in the IP address group will be added; existing ones will have their descriptions updated.
description	No	String	Provides remarks about the IP address group.

Response Parameters

Status code: 200

Table 5-265 Response body parameters

Parameter	Type	Description
ipgroup	**IpGroup** object	Shows the IP address group information.

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.

Table 5-266 IpGroup

Parameter	Type	Description
id	String	Specifies the ID of the IP address group.
name	String	Specifies the IP address group name.
description	String	Provides supplementary information about the IP address group.
ip_list	Array of **IpInfo** objects	Specifies the IP addresses or CIDR blocks in the IP address group. **[]** indicates any IP address.
listeners	Array of **ListenerRef** objects	Lists the IDs of listeners with which the IP address group is associated.
project_id	String	Specifies the project ID of the IP address group.
enterprise_project_id	String	Specifies the ID of the enterprise project that the IP address group belongs to.
created_at	String	Specifies the time when the IP address group was created.
updated_at	String	Specifies the time when the IP address group was updated.

Table 5-267 IpInfo

Parameter	Type	Description
ip	String	Specifies the IP addresses in the IP address group.
description	String	Provides remarks about the IP address group.

Table 5-268 ListenerRef

Parameter	Type	Description
id	String	Specifies the listener ID.

Example Requests

Updating IP addresses in an IP address group

```
PUT https://{ELB_Endpoint}/v3/45977fa2dbd7482098dd68d0d8970117/elb/ipgroups/
8722e0e0-9cc9-4490-9660-8c9a5732fbb0/iplist/create-or-update

{
  "ipgroup" : {
    "name" : "test_ipg",
    "ip_list" : [ {
      "ip" : "192.168.1.123",
      "description" : "test"
    }, {
      "ip" : "192.168.1.120",
      "description" : "test update ip0"
    } ]
  }
}
```

Example Responses

Status code: 200

Successful request.

```
{
  "request_id" : "46d0dcbec23987f1429491731dce0feb",
  "ipgroup" : {
    "id" : "353d6c3b-aca0-40b7-a059-fad8b20419e7",
    "name" : "test_ipg",
    "project_id" : "060576798a80d5762fafc01a9b5eedc7",
    "description" : "",
    "ip_list" : [ {
      "ip" : "192.168.1.120",
      "description" : "test update ip0"
    }, {
      "ip" : "192.168.1.122",
      "description" : "test update ip2"
    }, {
      "ip" : "192.168.1.123",
      "description" : "test"
    } ],
    "listeners" : [ {
      "id" : "acef0c4d-3bd5-4cd0-8d83-c53e5b1fd652"
    }, {
      "id" : "edb23879-5511-4412-8b7b-9574de7a1295"
    } ],
    "created_at" : "2021-11-29T10:40:30Z",
    "updated_at" : "2022-12-05T13:14:01Z"
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Updating IP addresses in an IP address group

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;

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

public class UpdateIpListSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdateIpListRequest request = new UpdateIpListRequest();
        request.withIpgroupId("{ipgroup_id}");
        UpdateIpListRequestBody body = new UpdateIpListRequestBody();
        List<UpadateIpGroupIpOption> listIpgroupIpList = new ArrayList<>();
        listIpgroupIpList.add(
            new UpadateIpGroupIpOption()
                .withIp("192.168.1.123")
                .withDescription("test")
        );
        listIpgroupIpList.add(
            new UpadateIpGroupIpOption()
                .withIp("192.168.1.120")
                .withDescription("test update ip0")
        );
        UpdateIpListOption ipgroupbody = new UpdateIpListOption();
        ipgroupbody.withName("test_ipg")
            .withIpList(listIpgroupIpList);
        body.withIpgroup(ipgroupbody);
        request.withBody(body);
        try {
            UpdateIpListResponse response = client.updateIpList(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

Updating IP addresses in an IP address group

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdateIpListRequest()
        request.ipgroup_id = "{ipgroup_id}"
        listIpListIpgroup = [
            UpadateIpGroupIpOption(
                ip="192.168.1.123",
                description="test"
            ),
            UpadateIpGroupIpOption(
                ip="192.168.1.120",
                description="test update ip0"
            )
        ]
        ipgroupbody = UpdateIpListOption(
            name="test_ipg",
            ip_list=listIpListIpgroup
        )
        request.body = UpdateIpListRequestBody(
            ipgroup=ipgroupbody
        )
        response = client.update_ip_list(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

Updating IP addresses in an IP address group

```
package main
```



```
import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdateIpListRequest{}
    request.IpgroupId = "{ipgroup_id}"
    descriptionIpList:= "test"
    descriptionIpList1:= "test update ip0"
    var listIpListIpgroup = []model.UpadateIpGroupIpOption{
        {
            Ip: "192.168.1.123",
            Description: &descriptionIpList,
        },
        {
            Ip: "192.168.1.120",
            Description: &descriptionIpList1,
        },
    }
    nameIpgroup:= "test_ipg"
    ipgroupbody := &model.UpdateIpListOption{
        Name: &nameIpgroup,
        IpList: &listIpListIpgroup,
    }
    request.Body = &model.UpdateIpListRequestBody{
        Ipgroup: ipgroupbody,
    }
    response, err := client.UpdateIpList(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	Successful request.

Error Codes

See **Error Codes**.

5.9.7 Deleting IP Addresses from an IP Address Group

Function

This API is used to delete IP addresses from an IP address group.

Calling Method

For details, see **Calling APIs**.

URI

POST /v3/{project_id}/elb/ipgroups/{ipgroup_id}/iplist/batch-delete

Table 5-269 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
ipgroup_id	Yes	String	Specifies the ID of the IP address group.

Request Parameters

Table 5-270 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	Specifies the token used for IAM authentication.

Table 5-271 Request body parameters

Parameter	Mandatory	Type	Description
ipgroup	No	**BatchDeleteIpListOption** object	Specifies IP addresses that will be deleted from an IP address group in batches.

Table 5-272 BatchDeleteIpListOption

Parameter	Mandatory	Type	Description
ip_list	No	Array of **IpGroupIp** objects	Specifies IP addresses.

Table 5-273 IpGroupIp

Parameter	Mandatory	Type	Description
ip	Yes	String	Specifies an IP address or IP address range.

Response Parameters

Status code: 200

Table 5-274 Response body parameters

Parameter	Type	Description
ipgroup	**IpGroup** object	Shows the IP address group information.
request_id	String	Specifies the request ID. Note: The value is automatically generated.

Table 5-275 IpGroup

Parameter	Type	Description
id	String	Specifies the ID of the IP address group.
name	String	Specifies the IP address group name.

Parameter	Type	Description
description	String	Provides supplementary information about the IP address group.
ip_list	Array of **IpInfo** objects	Specifies the IP addresses or CIDR blocks in the IP address group. **[]** indicates any IP address.
listeners	Array of **ListenerRef** objects	Lists the IDs of listeners with which the IP address group is associated.
project_id	String	Specifies the project ID of the IP address group.
enterprise_project_id	String	Specifies the ID of the enterprise project that the IP address group belongs to.
created_at	String	Specifies the time when the IP address group was created.
updated_at	String	Specifies the time when the IP address group was updated.

Table 5-276 IpInfo

Parameter	Type	Description
ip	String	Specifies the IP addresses in the IP address group.
description	String	Provides remarks about the IP address group.

Table 5-277 ListenerRef

Parameter	Type	Description
id	String	Specifies the listener ID.

Example Requests

Deleting IP addresses from an IP address group

```
PUT https://{ELB_Endpoint}/v3/45977fa2dbd7482098dd68d0d8970117/elb/ipgroups/
8722e0e0-9cc9-4490-9660-8c9a5732fbb0/iplist/batch-delete

{
  "ipgroup" : {
    "ip_list" : [ {
```



```
    "ip" : "192.168.1.123"
   }, {
    "ip" : "192.168.3.0/24"
   } ]
  }
}
```

Example Responses

Status code: 200

Successful request.

```
{
  "ipgroup" : {
    "description" : "",
    "id" : "8722e0e0-9cc9-4490-9660-8c9a5732fbb0",
    "name" : "test_ipg",
    "project_id" : "45977fa2dbd7482098dd68d0d8970117",
    "ip_list" : [ {
      "ip" : "192.168.1.122",
      "description" : ""
    } ],
    "listeners" : [ {
      "id" : "88f9c079-29cb-435a-b98f-0c5c0b90c2bd"
    }, {
      "id" : "2f4c9644-d5d2-4cf8-a3c0-944239a4f58c"
    } ],
    "created_at" : "2018-01-16T03:19:16",
    "updated_at" : "2018-01-16T03:19:16"
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Deleting IP addresses from an IP address group

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;

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

public class BatchDeleteIpListSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        BatchDeleteIpListRequest request = new BatchDeleteIpListRequest();
        request.withIpgroupId("{ipgroup_id}");
        BatchDeleteIpListRequestBody body = new BatchDeleteIpListRequestBody();
        List<IpGroupIp> listIpgroupIpList = new ArrayList<>();
        listIpgroupIpList.add(
            new IpGroupIp()
                .withIp("192.168.1.123")
        );
        listIpgroupIpList.add(
            new IpGroupIp()
                .withIp("192.168.3.0/24")
        );
        BatchDeleteIpListOption ipgroupbody = new BatchDeleteIpListOption();
        ipgroupbody.withIpList(listIpgroupIpList);
        body.withIpgroup(ipgroupbody);
        request.withBody(body);
        try {
            BatchDeleteIpListResponse response = client.batchDeleteIpList(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

Deleting IP addresses from an IP address group

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
```



```
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = BatchDeleteIpListRequest()
        request.ipgroup_id = "{ipgroup_id}"
        listIpListIpgroup = [
            IpGroupIp(
                ip="192.168.1.123"
            ),
            IpGroupIp(
                ip="192.168.3.0/24"
            )
        ]
        ipgroupbody = BatchDeleteIpListOption(
            ip_list=listIpListIpgroup
        )
        request.body = BatchDeleteIpListRequestBody(
            ipgroup=ipgroupbody
        )
        response = client.batch_delete_ip_list(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

Deleting IP addresses from an IP address group

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.BatchDeleteIpListRequest{}
    request.IpgroupId = "{ipgroup_id}"
    var listIpListIpgroup = []model.IpGroupIp{
        {
            Ip: "192.168.1.123",
```



```
        },
        {
            Ip: "192.168.3.0/24",
        },
    }
    ipgroupbody := &model.BatchDeleteIpListOption{
        IpList: &listIpListIpgroup,
    }
    request.Body = &model.BatchDeleteIpListRequestBody{
        Ipgroup: ipgroupbody,
    }
    response, err := client.BatchDeleteIpList(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	Successful request.

Error Codes

See **Error Codes**.

5.9.8 Querying the Listeners Associated with an IP Address Group

Function

This API is used to query the listeners associated with an IP address group.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/ipgroups/{ipgroup_id}/related-listeners

Table 5-278 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
ipgroup_id	Yes	String	Specifies the ID of an IP address group.

Request Parameters

Table 5-279 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-280 Response body parameters

Parameter	Type	Description
listeners	Array of **ListenerRef** objects	Specifies the IDs of all listeners associated with the IP address group.

Table 5-281 ListenerRef

Parameter	Type	Description
id	String	Specifies the listener ID.

Example Requests

Querying the listeners associated with an IP address group

```
GET https://{ELB_Endpoint}/v3/45977fa2dbd7482098dd68d0d8970117/elb/ipgroups/
8722e0e0-9cc9-4490-9660-8c9a5732fbb0/related-listeners
```

Example Responses

Status code: 200

Normal response to the operation.


```
{
  "listeners" : [ {
    "id" : "10000000-0000-0000-0000-000000000001"
  }, {
    "id" : "10000000-0000-0000-0000-000000000002"
  }, {
    "id" : "10000000-0000-0000-0000-000000000003"
  } ]
}
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ShowIpGroupRelatedListenersSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowIpGroupRelatedListenersRequest request = new ShowIpGroupRelatedListenersRequest();
        request.withIpgroupId("{ipgroup_id}");
        try {
            ShowIpGroupRelatedListenersResponse response = client.showIpGroupRelatedListeners(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowIpGroupRelatedListenersRequest()
        request.ipgroup_id = "{ipgroup_id}"
        response = client.show_ip_group_related_listeners(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
```



```
        WithCredential(auth).
        Build())

    request := &model.ShowIpGroupRelatedListenersRequest{}
    request.IpgroupId = "{ipgroup_id}"
    response, err := client.ShowIpGroupRelatedListeners(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 operation.

Error Codes

See **Error Codes**.

5.10 Listener

5.10.1 Adding a Listener

Function

This API is used to add a listener to a load balancer.

Constraints

When adding a listener, note the following:

- For load balancing at Layer 4, the listener protocol can be TCP, UDP, or TLS.
- For load balancing at Layer 7, the listener protocol can be HTTP, HTTPS or QUIC.
- For load balancing both at Layer 4 and Layer 7, the listener protocol can be TCP, UDP, TLS, HTTP, HTTPS, or QUIC.

Calling Method

For details, see **Calling APIs**.

URI

POST /v3/{project_id}/elb/listeners

Table 5-282 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Request Parameters

Table 5-283 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Table 5-284 Request body parameters

Parameter	Mandatory	Type	Description
listener	Yes	**CreateListenerOption** object	Specifies the listener.

Table 5-285 CreateListenerOption

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Specifies the administrative status of the listener. The value can only be **true**.
default_pool_id	No	String	Specifies the ID of the default backend server group. If there is no matched forwarding policy, requests will be forwarded to the default backend server for processing.

Parameter	Mandatory	Type	Description
client_ca_tls_container_ref	No	String	Specifies the ID of the CA certificate used by the listener. Note: • This parameter is available only when **type** is set to **client**. • This parameter is not available if the listener protocol is **QUIC**.
default_tls_container_ref	No	String	Specifies the ID of the server certificate used by the listener. This parameter is available only when the listener's protocol is HTTPS, TLS, or QUIC and **type** is set to **server**.
description	No	String	Provides supplementary information about the listener.
http2_enable	No	Boolean	Specifies whether to use HTTP/2 if you want the clients to use HTTP/2 to communicate with the load balancer. Request forwarding using HTTP/2 improves the access performance between your application and the load balancer. However, the load balancer still uses HTTP/1.x to forward requests to the backend server. Note: • This parameter is available only for HTTPS listeners. • If you configure this parameter for listeners with other protocols, it will not take effect. • For QUIC listeners, it cannot be set and the response is fixed at **true**.

Parameter	Mandatory	Type	Description
insert_headers	No	ListenerInsertHeaders object	Specifies the HTTP header fields that can transmit required information to backend servers. For example, the X-Forwarded-ELB-IP header field can transmit the EIP of the load balancer to backend servers.
loadbalancer_id	Yes	String	Specifies the ID of the load balancer that the listener is added to. Note: A listener can be added to only one load balancer.
name	No	String	Specifies the listener name. Note: If you leave the listener name empty, you cannot locate it on the listener list and view its details.
project_id	No	String	Specifies the project ID.
protocol	Yes	String	Specifies the protocol used by the listener. The value can be **TCP**, **UDP**, **HTTP**, **HTTPS**, **TERMINATED_HTTPS**, **QUIC**, or **TLS**. Note: • Protocol used by HTTPS listeners added to a shared load balancer can only be set to **TERMINATED_HTTPS**. If **HTTPS** is passed, the value will be automatically changed to **TERMINATED_HTTPS**. • Protocol used by HTTPS listeners added to a dedicated load balancer can only be set to **HTTPS**. If **TERMINATED_HTTPS** is passed, the value will be automatically changed to **HTTPS**.

Parameter	Mandatory	Type	Description
protocol_port	No	Integer	Specifies the port used by the listener. Note: • The QUIC listener port cannot be 4789 or the same as the UDP listener port. • If this parameter is set to **0**, **port_ranges** is required. • The port of HTTP or TERMINATED_HTTPS listeners added to a shared load balancer cannot be 21.
sni_container_refs	No	Array of strings	Specifies the IDs of SNI certificates (server certificates with domain names) used by the listener. Note: • The domain names of all SNI certificates must be unique. • The total number of domain names of all SNI certificates cannot exceed 50.
sni_match_algo	No	String	Specifies how wildcard domain name matches with the SNI certificates used by the listener. Value options: • **longest_suffix**: indicates longest suffix match. • **wildcard** (default): indicates wildcard match.
tags	No	Array of **Tag** objects	Lists the tags.

Parameter	Mandatory	Type	Description
tls_ciphers_policy	No	String	Specifies the security policy used by the listener. The value can be **tls-1-0-inherit**, **tls-1-0**, **tls-1-1**, **tls-1-2** (default), **tls-1-2-strict**, **tls-1-2-fs**, **tls-1-0-with-1-3**, **tls-1-2-fs-with-1-3**, **hybrid-policy-1-0**, or **tls-1-2-strict-no-cbc**. Note: • This parameter will take effect only for HTTPS listeners added to a dedicated load balancer. • This parameter is not available for QUIC listeners. • If both **security_policy_id** and **tls_ciphers_policy** are specified, only **security_policy_id** will take effect. • The encryption suite priority from the highest to lowest is ECC suite, RSA suite, and finally TLS 1.3 suite (supporting both ECC and RSA).

Parameter	Mandatory	Type	Description
security_policy_id	No	String	Specifies the ID of the custom security policy. Note: • This parameter will take effect only for HTTPS listeners added to a dedicated load balancer. • This parameter is not available for QUIC listeners. • If both **security_policy_id** and **tls_ciphers_policy** are specified, only **security_policy_id** will take effect. • The encryption suite priority from highest to lowest is ECC suite, RSA suite, and finally TLS 1.3 suite (supporting both ECC and RSA).
enable_member_retry	No	Boolean	Specifies whether to enable health check retries for backend servers. Value options: • **true** (default): Health check retries will be enabled. • **false**: Health check retries will be disabled. Note: • If a shared load balancer is associated, this parameter is available only when **protocol** is set to **HTTP** or **TERMINATED_HTTPS**. • If a dedicated load balancer is associated, this parameter is available only when **protocol** is set to **HTTP**, **HTTPS**, or **QUIC**.

Parameter	Mandatory	Type	Description
keepalive_timeout	No	Integer	Specifies the idle timeout duration, in seconds. If there are no requests reaching the load balancer after the idle timeout duration elapses, the load balancer will disconnect the connection with the client and establish a new connection when there is a new request. Value ranges: ● For TCP listeners, the value ranges from **10** to **4000**, and the default value is **300**. ● For HTTP, HTTPS, and TERMINATED_HTTPS listeners, the value ranges from **0** to **4000**, and the default value is **60**. Note: This parameter is not supported by UDP listeners of shared load balancers.
client_timeout	No	Integer	Specifies the timeout duration for waiting for a response from a client, in seconds. There are two situations: ● If the client fails to send a request header to the load balancer within the timeout duration, the request will be interrupted. ● If the interval between two consecutive request bodies reaching the load balancer is greater than the timeout duration, the connection will be disconnected. The value ranges from **1** to **300**, and the default value is **60**. This parameter is available only for HTTP and HTTPS listeners.

Parameter	Mandatory	Type	Description
member_timeout	No	Integer	Specifies the timeout duration for waiting for a response from a backend server, in seconds. If the backend server fails to respond after the timeout duration elapses, the load balancer will stop waiting and return HTTP 504 Gateway Timeout to the client. The value ranges from **1** to **300**, and the default value is **60**. This parameter is available only for HTTP and HTTPS listeners.
ipgroup	No	**CreateListenerIpGroupOption** object	Specifies the IP address group associated with the listener. The value can be **null**, or left blank, or be an empty JSON structure ({}), indicating that no IP address group is associated with the listener. **ipgroup_id** is also required if you want to associate an IP address group with the listener.

Parameter	Mandatory	Type	Description
transparent_client_ip_enable	No	Boolean	Specifies whether to pass source IP addresses of the clients to backend servers. Value options: • TCP or UDP listeners of shared load balancers: The value can be **true** or **false**, and the default value is **false** if this parameter is not passed. • HTTP or HTTPS listeners of shared load balancers: The value can only be **true**, and the default value is **true** if this parameter is not passed. • All listeners of dedicated load balancers: The value can only be **true**, and the default value is **true** if this parameter is not passed. Note: • This function can only be enabled or disabled for TCP or UDP listeners of shared load balancers. • If this function is enabled, the load balancer communicates with backend servers using their real IP addresses. Ensure that security group rules and access control policies are correctly configured. • If this function is enabled, a server cannot serve as both a backend server and a client. • If this function is enabled, backend server specifications cannot be changed.

Parameter	Mandatory	Type	Description
proxy_protocol_enable	No	Boolean	Specifies whether to enable the ProxyProtocol option to pass the source IP addresses of the clients to backend servers. Note: This parameter is available only for TLS listeners and does not take effect for other types of listeners.

Parameter	Mandatory	Type	Description
enhance_l7policy_enable	No	Boolean	Specifies whether to enable advanced forwarding. If advanced forwarding is enabled, more flexible forwarding policies and rules are supported. Value options: • **true**: Enable advanced forwarding. • **false** (default): Disable advanced forwarding. The following scenarios are supported: • **action** can be set to **REDIRECT_TO_URL** (requests will be redirected to another URL) or **Fixed_RESPONSE** (a fixed response body will be returned to clients). • Parameters **priority**, **redirect_url_config**, and **fixed_response_config** can be specified in a forwarding policy. • **type** can be set to **METHOD**, **HEADER**, **QUERY_STRING**, or **SOURCE_IP** for a forwarding rule. • If **type** is set to **HOST_NAME** for a forwarding rule, the value of the forwarding rule supports wildcard asterisks (*). • Parameter **conditions** can be specified for forwarding rules. Note: • Advanced forwarding cannot be disabled once it is enabled. • If advanced forwarding is enabled, forwarding policy priorities are defined by

Parameter	Mandatory	Type	Description
			priority. For details, see the description of the **priority** field in the forwarding policy.
quic_config	No	**CreateListenerQuicConfigOption** object	Specifies the QUIC configuration for the current listener. Note: • This parameter is valid only when **protocol** is set to **HTTPS**. For a TCP, UDP, HTTP, or QUIC listener, if this parameter is not left blank, an error will be reported. • The client sends a normal HTTP request that contains information indicating that the QUIC protocol is supported. If QUIC upgrade is enabled for the listeners, QUIC port and version information will be added to the response header. When the client sends both HTTPS and QUIC requests to the server, if the QUIC request is successfully sent, QUIC protocol will be used for subsequent communications.
protection_status	No	String	Specifies the protection status. Value options: • **nonProtection** (default): The load balancer is not protected. • **consoleProtection**: **Modification Protection** is enabled on the console.

Parameter	Mandatory	Type	Description
protection_reason	No	String	Specifies why the modification protection is enabled. Note: This parameter is valid only when **protection_status** is set to **consoleProtection**. The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).
gzip_enable	No	Boolean	Specifies whether to enable **gzip_enable** for a load balancer. The value can be **true** or **false**, and the default value is **false**. Note: This parameter can be configured only for HTTP, HTTPS, and QUIC listeners.
port_ranges	No	Array of **PortRange** objects	Specifies the port range, including the start and end port numbers. Note: • A maximum of 10 port ranges can be specified. The port range cannot overlap with each other. • This parameter can be specified only when **protocol_port** is set to **0** or **protocol_port** is not specified. • This parameter is available for TCP, UDP, or TLS listeners.

Parameter	Mandatory	Type	Description
ssl_early_data_enable	No	Boolean	Specifies whether to enable zero round trip time resumption (0-RTT) for listeners. Value options: **true** or **false** Default value: **false** This option can be configured only for HTTPS listeners and depends on the TLS 1.3 security policy protocols. If **ssl_early_data** is set to **true**, replay attacks may occur. Exercise caution when enabling this option.
cps	No	Integer	Specifies the maximum number of new connections that a listener can handle per second. Value range: **0** to **1000000** Default value: **0**, indicating that the number is not limited. Note: If the value is greater than the number defined in the load balancer specifications, the latter is used as the limit.
connection	No	Integer	Specifies the maximum number of concurrent connections that a listener can handle per second. Value range: **0** to **1000000** Default value: **0**, indicating that the number is not limited. Note: If the value is greater than the number defined in the load balancer specifications, the latter is used as the limit.

Parameter	Mandatory	Type	Description
nat64_enable	No	Boolean	Specifies whether to enable **nat64_enable**. This function enables a client to access IPv4 or IPv6 backend servers by accessing the IPv4 or IPv6 address of a load balancer. Constraints: This option can only be enabled for TCP and UDP listeners. **nat64_enable** is mutually exclusive with **transparent_client_ip_enable**. Value options: **true**: Enable **nat64_enable**. **false**: Disable **nat64_enable**. Default value: **false**

Table 5-286 ListenerInsertHeaders

Parameter	Mandatory	Type	Description
X-Forwarded-ELB-IP	No	Boolean	Specifies whether to transparently transmit the load balancer EIP to backend servers. If **X-Forwarded-ELB-IP** is set to **true**, the load balancer EIP will be stored in the HTTP header and passed to backend servers.
X-Forwarded-Port	No	Boolean	Specifies whether to transparently transmit the listening port of the load balancer to backend servers. If **X-Forwarded-Port** is set to **true**, the listening port of the load balancer will be stored in the HTTP header and passed to backend servers.

Parameter	Mandatory	Type	Description
X-Forwarded-For-Port	No	Boolean	Specifies whether to transparently transmit the source port of the client to backend servers. If **X-Forwarded-For-Port** is set to **true**, the source port of the client will be stored in the HTTP header and passed to backend servers.
X-Forwarded-Host	No	Boolean	Specifies whether to rewrite the **X-Forwarded-Host** header. If **X-Forwarded-Host** is set to **true**, **X-Forwarded-Host** in the request header from the clients can be set to **Host** in the request header sent from the load balancer to backend servers.
X-Forwarded-Proto	No	Boolean	If **X-Forwarded-Proto** is set to **true**, the listener protocol of the load balancer can be transferred to backend servers through the HTTP header of the packet.
X-Real-IP	No	Boolean	If **X-Real-IP** is set to **true**, the source IP address of the client can be transferred to backend servers through the HTTP header of the packet.
X-Forwarded-ELB-ID	No	Boolean	If **X-Forwarded-ELB-ID** is set to **true**, the load balancer ID can be transferred to backend servers through the HTTP header of the packet.
X-Forwarded-TLS-Certificate-ID	No	Boolean	If **X-Forwarded-TLS-Certificate-ID** is set to **true**, the certificate ID of the load balancer can be transferred to backend servers through the HTTP header of the packet.
X-Forwarded-TLS-Protocol	No	Boolean	If **X-Forwarded-TLS-Protocol** is set to **true**, the algorithm protocol of the load balancer can be transferred to backend servers through the HTTP header of the packet.

Parameter	Mandatory	Type	Description
X-Forwarded-TLS-Cipher	No	Boolean	If **X-Forwarded-TLS-Cipher** is set to **true**, the algorithm suite of the load balancer can be transferred to backend servers through the HTTP header of the packet.

Table 5-287 Tag

Parameter	Mandatory	Type	Description
key	No	String	Specifies the tag key.
value	No	String	Specifies the tag value.

Table 5-288 CreateListenerIpGroupOption

Parameter	Mandatory	Type	Description
ipgroup_id	Yes	String	Specifies the ID of the IP address group associated with the listener. Note: • If **ip_list** is set to an empty array **[]** and **type** to **whitelist**, no IP addresses are allowed to access the listener. • If **ip_list** is set to an empty array **[]** and **type** to **blacklist**, any IP address is allowed to access the listener.
enable_ipgroup	No	Boolean	Specifies whether access control is enabled. Value options: • **true**: Access control is enabled. • **false**: Access control is disabled.

Parameter	Mandatory	Type	Description
type	No	String	Specifies how access to the listener is controlled. Value options: • **white** (default): A whitelist will be configured. Only IP addresses in the whitelist can access the listener. • **black**: A blacklist will be configured. IP addresses in the blacklist are not allowed to access the listener.

Table 5-289 CreateListenerQuicConfigOption

Parameter	Mandatory	Type	Description
quic_listener_id	Yes	String	Specifies the ID of the QUIC listener. This parameter is mandatory for creation and is optional for update. The listener specified by **quic_listener_id** must exist. The listener protocol must be **QUIC** and cannot be set to **null**, otherwise, it will conflict with **enable_quic_upgrade**.
enable_quic_upgrade	No	Boolean	Specifies whether to enable QUIC upgrade. Value options: • **true**: QUIC upgrade is enabled. • **false**: QUIC upgrade is disabled. HTTPS listeners can be upgraded to QUIC listeners.

Table 5-290 PortRange

Parameter	Mandatory	Type	Description
start_port	No	Integer	Specifies the start port number.

Parameter	Mandatory	Type	Description
end_port	No	Integer	Specifies the end port number. The value must be greater than or equal to the start port number.

Response Parameters

Status code: 201

Table 5-291 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
listener	**Listener** object	Specifies the listener.

Table 5-292 Listener

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the listener.
client_ca_tls_container_ref	String	Specifies the ID of the CA certificate used by the listener. Note: This parameter is available only when **type** is set to **client**.
connection_limit	Integer	Specifies the maximum number of connections that the load balancer can establish with backend servers. **-1** indicates that the number of connections is not limited. Default value: **-1** This parameter is unsupported. Please do not use it.
created_at	String	Specifies the time when the listener was created, in the format of *yyyy-MM-dd''T''HH:mm:ss''Z''*, for example, 2021-07-30T12:03:44Z.

Parameter	Type	Description
default_pool_id	String	Specifies the ID of the default backend server group. If there is no matched forwarding policy, requests are forwarded to the default backend server.
default_tls_container_ref	String	Specifies the ID of the server certificate used by the listener.
description	String	Provides supplementary information about the listener.
http2_enable	Boolean	Specifies whether to use HTTP/2 if you want the clients to use HTTP/2 to communicate with the load balancer. Request forwarding using HTTP/2 improves the access performance between your application and the load balancer. However, the load balancer still uses HTTP/1.x to forward requests to the backend server. Note: • This parameter is available only for HTTPS listeners. • If you configure this parameter for listeners with other protocols, it will not take effect. • For QUIC listeners, it cannot be set and the response is fixed at **true**.
id	String	Specifies the listener ID.
insert_headers	**ListenerInsertHeaders** object	Specifies the HTTP header fields that can transmit required information to backend servers. For example, the X-Forwarded-ELB-IP header field can transmit the EIP of the load balancer to backend servers.
loadbalancers	Array of **LoadBalancerRef** objects	Specifies the ID of the load balancer that the listener is added to. A listener can be added to only one load balancer.
name	String	Specifies the listener name. Note: If you leave the listener name empty, you cannot locate it on the listener list and view its details.
project_id	String	Specifies the ID of the project where the listener is used.

Parameter	Type	Description
enterprise_project_id	String	Specifies the ID of the enterprise project.
protocol	String	Specifies the protocol used by the listener. The value can be **TCP**, **UDP**, **HTTP**, **HTTPS**, **TERMINATED_HTTPS**, **QUIC**, or **TLS**. Note: • Protocol used by HTTPS listeners added to a shared load balancer can only be set to **TERMINATED_HTTPS**. If **HTTPS** is passed, the value will be automatically changed to **TERMINATED_HTTPS**. • Protocol used by HTTPS listeners added to a dedicated load balancer can only be set to **HTTPS**. If **TERMINATED_HTTPS** is passed, the value will be automatically changed to **HTTPS**.
protocol_port	Integer	Specifies the port used by the listener. Note: • The QUIC listener port cannot be 4789 or the same as the UDP listener port. • If this parameter is set to **0**, **port_ranges** is required.
sni_container_refs	Array of strings	Specifies the IDs of SNI certificates (server certificates with domain names) used by the listener. Note: • The domain names of all SNI certificates must be unique. • The total number of domain names of all SNI certificates cannot exceed 50.

Parameter	Type	Description
sni_match_algo	String	Specifies how wildcard domain name matches with the SNI certificates used by the listener. Value options: • **longest_suffix**: indicates longest suffix match. • **wildcard** (default): indicates wildcard match.
tags	Array of **Tag** objects	Lists the tags.
updated_at	String	Specifies the time when the listener was updated, in the format of *yyyy-MM-dd''T''HH:mm:ss''Z''*, for example, 2021-07-30T12:03:44Z.
tls_ciphers_policy	String	Specifies the security policy used by the listener. The value can be **tls-1-0-inherit**, **tls-1-0**, **tls-1-1**, **tls-1-2** (default), **tls-1-2-strict**, **tls-1-2-fs**, **tls-1-0-with-1-3**, **tls-1-2-fs-with-1-3**, **hybrid-policy-1-0**, or **tls-1-2-strict-no-cbc**. Note: • This parameter will take effect only for HTTPS listeners added to a dedicated load balancer. • This parameter is not available for QUIC listeners. • If both **security_policy_id** and **tls_ciphers_policy** are specified, only **security_policy_id** will take effect. • The encryption suite priority from the highest to lowest is ECC suite, RSA suite, and finally TLS 1.3 suite (supporting both ECC and RSA).

Parameter	Type	Description
security_policy_id	String	Specifies the ID of the custom security policy. Note: • This parameter will take effect only for HTTPS listeners added to a dedicated load balancer. • This parameter is not available for QUIC listeners. • If both **security_policy_id** and **tls_ciphers_policy** are specified, only **security_policy_id** will take effect. • The encryption suite priority from highest to lowest is ECC suite, RSA suite, and finally TLS 1.3 suite (supporting both ECC and RSA).
enable_member_retry	Boolean	Specifies whether to enable health check retries for backend servers. Value options: • **true** (default): Health check retries will be enabled. • **false**: Health check retries will be disabled. Note: • If a shared load balancer is associated, this parameter is available only when **protocol** is set to **HTTP** or **TERMINATED_HTTPS**. • If a dedicated load balancer is associated, this parameter is available only when **protocol** is set to **HTTP**, **HTTPS**, or **QUIC**.

Parameter	Type	Description
keepalive_timeout	Integer	Specifies the idle timeout duration, in seconds. If there are no requests reaching the load balancer after the idle timeout duration elapses, the load balancer will disconnect the connection with the client and establish a new connection when there is a new request. Value ranges: • For TCP listeners, the value ranges from **10** to **4000**, and the default value is **300**. • For HTTP, HTTPS, and TERMINATED_HTTPS listeners, the value ranges from **0** to **4000**, and the default value is **60**. Note: This parameter is not supported by UDP listeners of shared load balancers.
client_timeout	Integer	Specifies the timeout duration for waiting for a response from a client, in seconds. There are two situations: • If the client fails to send a request header to the load balancer within the timeout duration, the request will be interrupted. • If the interval between two consecutive request bodies reaching the load balancer is greater than the timeout duration, the connection will be disconnected. The value ranges from **1** to **300**, and the default value is **60**. This parameter is available only for HTTP and HTTPS listeners.

Parameter	Type	Description
member_timeout	Integer	Specifies the timeout duration for waiting for a response from a backend server, in seconds. If the backend server fails to respond after the timeout duration elapses, the load balancer will stop waiting and return HTTP 504 Gateway Timeout to the client. The value ranges from **1** to **300**, and the default value is **60**. This parameter is available only for HTTP and HTTPS listeners.
ipgroup	**ListenerIpGroup** object	Specifies the IP address group associated with the listener.
transparent_client_ip_enable	Boolean	Specifies whether to pass source IP addresses of the clients to backend servers. Value options: • TCP or UDP listeners of shared load balancers: The value can be **true** or **false**, and the default value is **false** if this parameter is not passed. • HTTP or HTTPS listeners of shared load balancers: The value can only be **true**, and the default value is **true** if this parameter is not passed. • All listeners of dedicated load balancers: The value can only be **true**, and the default value is **true** if this parameter is not passed. Note: • This function can only be enabled or disabled for TCP or UDP listeners of shared load balancers. • If this function is enabled, the load balancer communicates with backend servers using their real IP addresses. Ensure that security group rules and access control policies are correctly configured. • If this function is enabled, a server cannot serve as both a backend server and a client. • If this function is enabled, backend server specifications cannot be changed.

Parameter	Type	Description
proxy_protocol_enable	Boolean	Specifies whether to enable the ProxyProtocol option to pass the source IP addresses of the clients to backend servers. Note: This parameter is available only for TLS listeners and does not take effect for other types of listeners.
enhance_l7policy_enable	Boolean	Specifies whether to enable advanced forwarding. If advanced forwarding is enabled, more flexible forwarding policies and rules are supported. Value options: • **true**: Enable advanced forwarding. • **false** (default): Disable advanced forwarding. The following scenarios are supported: • **action** can be set to **REDIRECT_TO_URL** (requests will be redirected to another URL) or **FIXED_RESPONSE** (a fixed response body will be returned to clients). • Parameters **priority**, **redirect_url_config**, and **fixed_response_config** can be specified in a forwarding policy. • **type** can be set to **METHOD**, **HEADER**, **QUERY_STRING**, or **SOURCE_IP** for a forwarding rule. • If **type** is set to **HOST_NAME** for a forwarding rule, the value of the forwarding rule supports wildcard asterisks (*). • Parameter **conditions** can be specified for forwarding rules. Note: • Advanced forwarding cannot be disabled once it is enabled. • If advanced forwarding is enabled, forwarding policy priorities are defined by **priority**. For details, see the description of the **priority** field in the forwarding policy.

Parameter	Type	Description
quic_config	**ListenerQuicConfig** object	Specifies the QUIC configuration for the current listener. Note: • This parameter is valid only when **protocol** is set to **HTTPS**. For a TCP, UDP, HTTP, or QUIC listener, if this parameter is not left blank, an error will be reported. • The client sends a normal HTTP request that contains information indicating that the QUIC protocol is supported. If QUIC upgrade is enabled for the listeners, QUIC port and version information will be added to the response header. When the client sends both HTTPS and QUIC requests to the server, if the QUIC request is successfully sent, QUIC protocol will be used for subsequent communications.
protection_status	String	Specifies the protection status. Value options: • **nonProtection** (default): The load balancer is not protected. • **consoleProtection**: **Modification Protection** is enabled on the console.
protection_reason	String	Specifies why the modification protection is enabled. Note: This parameter is valid only when **protection_status** is set to **consoleProtection**. The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).
gzip_enable	Boolean	Specifies whether to enable gzip compression for a load balancer. The value can be **true** or **false**, and the default value is **false**. Note: This parameter can be configured only for HTTP, HTTPS, and QUIC listeners.

Parameter	Type	Description
port_ranges	Array of **PortRange** objects	Specifies the port range, including the start and end port numbers. Note: • A maximum of 10 port ranges can be specified. The port range cannot overlap with each other. • This parameter can be specified only when **protocol_port** is set to **0**.
ssl_early_data_enable	Boolean	Specifies whether to enable zero round trip time resumption (0-RTT) for listeners. The default value is **false**. This option can be configured only for HTTPS listeners and depends on the TLS 1.3 security policy protocols.
cps	Integer	Specifies the maximum number of new connections that a listener can handle per second. Value range: **0** to **1000000** Default value: **0**, indicating that the number is not limited. Note: If the value is greater than the number defined in the load balancer specifications, the latter is used as the limit.
connection	Integer	Specifies the maximum number of concurrent connections that a listener can handle per second. Value range: **0** to **1000000** Default value: **0**, indicating that the number is not limited. Note: If the value is greater than the number defined in the load balancer specifications, the latter is used as the limit.

Parameter	Type	Description
nat64_enable	Boolean	Specifies whether to enable **nat64_enable**. This function enables a client to access IPv4 or IPv6 backend servers by accessing the IPv4 or IPv6 address of a load balancer. Constraints: This option can only be enabled for TCP and UDP listeners. **nat64_enable** is mutually exclusive with **transparent_client_ip_enable**. Value options: **true**: Enable **nat64_enable**. **false**: Disable **nat64_enable**. Default value: **false**

Table 5-293 ListenerInsertHeaders

Parameter	Type	Description
X-Forwarded-ELB-IP	Boolean	Specifies whether to transparently transmit the load balancer EIP to backend servers. If **X-Forwarded-ELB-IP** is set to **true**, the load balancer EIP will be stored in the HTTP header and passed to backend servers.
X-Forwarded-Port	Boolean	Specifies whether to transparently transmit the listening port of the load balancer to backend servers. If **X-Forwarded-Port** is set to **true**, the listening port of the load balancer will be stored in the HTTP header and passed to backend servers.
X-Forwarded-For-Port	Boolean	Specifies whether to transparently transmit the source port of the client to backend servers. If **X-Forwarded-For-Port** is set to **true**, the source port of the client will be stored in the HTTP header and passed to backend servers.
X-Forwarded-Host	Boolean	Specifies whether to rewrite the **X-Forwarded-Host** header. If **X-Forwarded-Host** is set to **true**, **X-Forwarded-Host** in the request header from the clients can be set to **Host** in the request header sent from the load balancer to backend servers.

Parameter	Type	Description
X-Forwarded-Proto	Boolean	If **X-Forwarded-Proto** is set to **true**, the listener protocol of the load balancer can be transferred to backend servers through the HTTP header of the packet.
X-Real-IP	Boolean	If **X-Real-IP** is set to **true**, the source IP address of the client can be transferred to backend servers through the HTTP header of the packet.
X-Forwarded-ELB-ID	Boolean	If **X-Forwarded-ELB-ID** is set to **true**, the load balancer ID can be transferred to backend servers through the HTTP header of the packet.
X-Forwarded-TLS-Certificate-ID	Boolean	If **X-Forwarded-TLS-Certificate-ID** is set to **true**, the certificate ID of the load balancer can be transferred to backend servers through the HTTP header of the packet.
X-Forwarded-TLS-Protocol	Boolean	If **X-Forwarded-TLS-Protocol** is set to **true**, the algorithm protocol of the load balancer can be transferred to backend servers through the HTTP header of the packet.
X-Forwarded-TLS-Cipher	Boolean	If **X-Forwarded-TLS-Cipher** is set to **true**, the algorithm suite of the load balancer can be transferred to backend servers through the HTTP header of the packet.

Table 5-294 LoadBalancerRef

Parameter	Type	Description
id	String	Specifies the load balancer ID.

Table 5-295 Tag

Parameter	Type	Description
key	String	Specifies the tag key.
value	String	Specifies the tag value.

Table 5-296 ListenerIpGroup

Parameter	Type	Description
ipgroup_id	String	Specifies the ID of the IP address group associated with the listener. This parameter is mandatory when you create the IP address group and is optional when you update the IP address group. Note: The specified IP address group must exist, and the value cannot be **null**.
enable_ipgroup	Boolean	Specifies whether access control is enabled. Value options: • **true**: Access control is enabled. • **false**: Access control is disabled. A listener with access control enabled can be directly deleted.
type	String	Specifies how access to the listener is controlled. Value options: • **white** (default): A whitelist will be configured. Only IP addresses in the whitelist can access the listener. • **black**: A blacklist will be configured. IP addresses in the blacklist are not allowed to access the listener.

Table 5-297 ListenerQuicConfig

Parameter	Type	Description
quic_listener_id	String	Specifies the ID of the QUIC listener. This parameter is mandatory for creation and is optional for update. The listener specified by **quic_listener_id** must exist. The listener protocol must be **QUIC** and cannot be set to **null**, otherwise, it will conflict with **enable_quic_upgrade**.

Parameter	Type	Description
enable_quic_upgrade	Boolean	Specifies whether to enable QUIC upgrade. Value options: • **true**: QUIC upgrade is enabled. • **false**: QUIC upgrade is disabled. HTTPS listeners can be upgraded to QUIC listeners.

Table 5-298 PortRange

Parameter	Type	Description
start_port	Integer	Specifies the start port number.
end_port	Integer	Specifies the end port number. The value must be greater than or equal to the start port number.

Example Requests

- Example 1: Adding a TCP listener

```
POST https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/listeners

{
  "listener" : {
    "protocol_port" : 80,
    "protocol" : "TCP",
    "loadbalancer_id" : "098b2f68-af1c-41a9-8efd-69958722af62",
    "name" : "My listener",
    "admin_state_up" : true,
    "insert_headers" : {
      "X-Forwarded-ELB-IP" : true
    }
  }
}
```

- Example 2: Adding an HTTPS listener

```
POST https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/listeners

{
  "listener" : {
    "protocol_port" : 90,
    "protocol" : "HTTPS",
    "loadbalancer_id" : "098b2f68-af1c-41a9-8efd-69958722af62",
    "name" : "My listener",
    "admin_state_up" : true,
    "ipgroup" : {
      "ipgroup_id" : "0416b6f1-877f-4a51-987e-978b3f083542",
      "type" : "black"
    },
    "security_policy_id" : "8722e0e0-9cc9-4490-9660-8c9a5732fbb0",
    "default_tls_container_ref" : "233a325e5e3e4ce8beeb320aa714cc12"
  }
}
```


Example Responses

Status code: 201

Normal response to POST requests.


```
{
  "listener" : {
    "id" : "0b11747a-b139-492f-9692-2df0b1c87193",
    "name" : "My listener",
    "protocol_port" : 80,
    "protocol" : "TCP",
    "description" : null,
    "default_tls_container_ref" : null,
    "admin_state_up" : true,
    "loadbalancers" : [ {
      "id" : "098b2f68-af1c-41a9-8efd-69958722af62"
    } ],
    "client_ca_tls_container_ref" : null,
    "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
    "sni_container_refs" : [ ],
    "connection_limit" : -1,
    "member_timeout" : null,
    "client_timeout" : null,
    "keepalive_timeout" : null,
    "default_pool_id" : null,
    "ipgroup" : null,
    "tls_ciphers_policy" : "tls-1-2",
    "tags" : [ ],
    "created_at" : "2019-04-02T00:12:32Z",
    "updated_at" : "2019-04-02T00:12:32Z",
    "http2_enable" : false,
    "enable_member_retry" : true,
    "insert_headers" : {
      "X-Forwarded-ELB-IP" : true
    },
    "transparent_client_ip_enable" : false,
    "nat64_enable" : false
  },
  "request_id" : "f4c4aca8-df16-42e8-8836-33e4b8e9aa8e"
}
```


SDK Sample Code

The SDK sample code is as follows.

Java

- Example 1: Adding a TCP listener

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class CreateListenerSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateListenerRequest request = new CreateListenerRequest();
        CreateListenerRequestBody body = new CreateListenerRequestBody();
        ListenerInsertHeaders insertHeadersListener = new ListenerInsertHeaders();
        insertHeadersListener.withXForwardedELBIP(true);
        CreateListenerOption listenerbody = new CreateListenerOption();
        listenerbody.withAdminStateUp(true)
            .withInsertHeaders(insertHeadersListener)
            .withLoadbalancerId("098b2f68-af1c-41a9-8efd-69958722af62")
            .withName("My listener")
            .withProtocol("TCP")
            .withProtocolPort(80);
        body.withListener(listenerbody);
        request.withBody(body);
        try {
            CreateListenerResponse response = client.createListener(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());
        }
    }
}
```

- Example 2: Adding an HTTPS listener

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class CreateListenerSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateListenerRequest request = new CreateListenerRequest();
        CreateListenerRequestBody body = new CreateListenerRequestBody();
        CreateListenerIpGroupOption ipgroupListener = new CreateListenerIpGroupOption();
        ipgroupListener.withIpgroupId("0416b6f1-877f-4a51-987e-978b3f083542")
            .withType(CreateListenerIpGroupOption.TypeEnum.fromValue("black"));
        CreateListenerOption listenerbody = new CreateListenerOption();
        listenerbody.withAdminStateUp(true)
            .withDefaultTlsContainerRef("233a325e5e3e4ce8beeb320aa714cc12")
            .withLoadbalancerId("098b2f68-af1c-41a9-8efd-69958722af62")
            .withName("My listener")
            .withProtocol("HTTPS")
            .withProtocolPort(90)
            .withSecurityPolicyId("8722e0e0-9cc9-4490-9660-8c9a5732fbb0")
            .withIpgroup(ipgroupListener);
        body.withListener(listenerbody);
        request.withBody(body);
        try {
            CreateListenerResponse response = client.createListener(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

- Example 1: Adding a TCP listener

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
```



```
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateListenerRequest()
        insertHeadersListener = ListenerInsertHeaders(
            x_forwarded_elb_ip=True
        )
        listenerbody = CreateListenerOption(
            admin_state_up=True,
            insert_headers=insertHeadersListener,
            loadbalancer_id="098b2f68-af1c-41a9-8efd-69958722af62",
            name="My listener",
            protocol="TCP",
            protocol_port=80
        )
        request.body = CreateListenerRequestBody(
            listener=listenerbody
        )
        response = client.create_listener(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

- Example 2: Adding an HTTPS listener

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateListenerRequest()
        ipgroupListener = CreateListenerIpGroupOption(
            ipgroup_id="0416b6f1-877f-4a51-987e-978b3f083542",
            type="black"
        )
        listenerbody = CreateListenerOption(
            admin_state_up=True,
            default_tls_container_ref="233a325e5e3e4ce8beeb320aa714cc12",
            loadbalancer_id="098b2f68-af1c-41a9-8efd-69958722af62",
            name="My listener",
            protocol="HTTPS",
            protocol_port=90,
            security_policy_id="8722e0e0-9cc9-4490-9660-8c9a5732fbb0",
            ipgroup=ipgroupListener
```



```
        )
        request.body = CreateListenerRequestBody(
            listener=listenerbody
        )
        response = client.create_listener(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

- Example 1: Adding a TCP listener

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateListenerRequest{}
    xForwardedELBIPInsertHeaders:= true
    insertHeadersListener := &model.ListenerInsertHeaders{
        XForwardedELBIP: &xForwardedELBIPInsertHeaders,
    }
    adminStateUpListener:= true
    nameListener:= "My listener"
    protocolPortListener:= int32(80)
    listenerbody := &model.CreateListenerOption{
        AdminStateUp: &adminStateUpListener,
        InsertHeaders: insertHeadersListener,
        LoadbalancerId: "098b2f68-af1c-41a9-8efd-69958722af62",
        Name: &nameListener,
        Protocol: "TCP",
        ProtocolPort: &protocolPortListener,
    }
    request.Body = &model.CreateListenerRequestBody{
        Listener: listenerbody,
    }
    response, err := client.CreateListener(request)
    if err == nil {
```



```
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

- Example 2: Adding an HTTPS listener

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateListenerRequest{}
    typeIpgroup:= model.GetCreateListenerIpGroupOptionTypeEnum().BLACK
    ipgroupListener := &model.CreateListenerIpGroupOption{
        IpgroupId: "0416b6f1-877f-4a51-987e-978b3f083542",
        Type: &typeIpgroup,
    }
    adminStateUpListener:= true
    defaultTlsContainerRefListener:= "233a325e5e3e4ce8beeb320aa714cc12"
    nameListener:= "My listener"
    protocolPortListener:= int32(90)
    securityPolicyIdListener:= "8722e0e0-9cc9-4490-9660-8c9a5732fbb0"
    listenerbody := &model.CreateListenerOption{
        AdminStateUp: &adminStateUpListener,
        DefaultTlsContainerRef: &defaultTlsContainerRefListener,
        LoadbalancerId: "098b2f68-af1c-41a9-8efd-69958722af62",
        Name: &nameListener,
        Protocol: "HTTPS",
        ProtocolPort: &protocolPortListener,
        SecurityPolicyId: &securityPolicyIdListener,
        Ipgroup: ipgroupListener,
    }
    request.Body = &model.CreateListenerRequestBody{
        Listener: listenerbody,
    }
    response, err := client.CreateListener(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 POST requests.

Error Codes

See **Error Codes**.

5.10.2 Querying Listeners

Function

This API is used to query listeners.

Constraints

This API has the following constraints:

- Parameters **marker**, **limit**, and **page_reverse** are used for pagination query.
- Parameters **marker** and **page_reverse** take effect only when they are used together with parameter **limit**.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/listeners

Table 5-299 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Table 5-300 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Specifies the number of records on each page. Value range: 0–2000 Default value: 2000
marker	No	String	Specifies the ID of the last record on the previous page. Note: • This parameter must be used together with **limit**. • If this parameter is not specified, the first page will be queried. • This parameter cannot be left blank or set to an invalid ID.
page_reverse	No	Boolean	Specifies whether to use reverse query. Value options: • **true**: Query the previous page. • **false** (default): Query the next page. Note: • This parameter must be used together with **limit**. • If **page_reverse** is set to **true** and you want to query the previous page, set the value of **marker** to the value of **previous_marker**.
protocol_port	No	Array of strings	Specifies the port used by the listener. Multiple ports can be queried in the format of *protocol_port=xxx&protocol_port=xxx*.

Parameter	Mandatory	Type	Description
protocol	No	Array of strings	Specifies the protocol used by the listener. The value can be **TCP**, **UDP**, **HTTP**, **HTTPS**, **TERMINATED_HTTPS**, **QUIC**, or **TLS**. Multiple protocols can be queried in the format of *protocol=xxx&protocol=xxx*.
description	No	Array of strings	Provides supplementary information about the listener. Multiple descriptions can be queried in the format of *description=xxx&description=xxx*.
default_tls_container_ref	No	Array of strings	Specifies the ID of the server certificate used by the listener. Multiple IDs can be queried in the format of *default_tls_container_ref=xxx&default_tls_container_ref=xxx*.
client_ca_tls_container_ref	No	Array of strings	Specifies the ID of the CA certificate used by the listener. Multiple IDs can be queried in the format of *client_ca_tls_container_ref=xxx&client_ca_tls_container_ref=xxx*.
admin_state_up	No	Boolean	Specifies the administrative status of the listener.
connection_limit	No	Array of integers	Specifies the maximum number of connections that the load balancer can establish with backend servers. The value **-1** indicates that the number of connections is not limited. Multiple values can be queried in the format of *connection_limit=xxx&connection_limit=xxx*. This parameter is unsupported. Please do not use it.

Parameter	Mandatory	Type	Description
default_pool_id	No	Array of strings	Specifies the ID of the default backend server group. If there is no matched forwarding policy, requests will be routed to the default backend server. Multiple IDs can be queried in the format of *default_pool_id=xxx&default_pool_id=xxx*.
id	No	Array of strings	Specifies the listener ID. Multiple IDs can be queried in the format of *id=xxx&id=xxx*.
name	No	Array of strings	Specifies the name of the listener added to the load balancer. Multiple names can be queried in the format of *name=xxx&name=xxx*.
http2_enable	No	Boolean	Specifies whether to use HTTP/2 if you want the clients to use HTTP/2 to communicate with the load balancer. Request forwarding using HTTP/2 improves the access performance between your application and the load balancer. However, the load balancer still uses HTTP/1.x to forward requests to the backend server. Note: • This parameter is available only for HTTPS listeners. • If you configure this parameter for listeners with other protocols, it will not take effect. • For QUIC listeners, it cannot be set and the response is fixed at **true**.

Parameter	Mandatory	Type	Description
loadbalancer_id	No	Array of strings	Specifies the ID of the load balancer that the listener is added to. Multiple IDs can be queried in the format of *loadbalancer_id=xxx&loadbalancer_id=xxx*.
tls_ciphers_policy	No	Array of strings	Specifies the security policy used by the listener. Multiple security policies can be queried in the format of *tls_ciphers_policy=xxx&tls_ciphers_policy=xxx*.
member_address	No	Array of strings	Specifies the private IP address bound to the backend server. This parameter is used only as a query condition and is not included in the response. Multiple IP addresses can be queried in the format of *member_address=xxx&member_address=xxx*.
member_device_id	No	Array of strings	Specifies the ID of the cloud server that serves as a backend server. This parameter is used only as a query condition and is not included in the response. Multiple IDs can be queried in the format of *member_device_id=xxx&member_device_id=xxx*.

Parameter	Mandatory	Type	Description
enterprise_project_id	No	Array of strings	Specifies the ID of the enterprise project. • If **enterprise_project_id** is not specified, resources in all enterprise projects are queried by default. Fine-grained authorization is performed. The **elb:listeners:list** permission must be assigned to the user group. • If **enterprise_project_id** is specified, the value can be a specific enterprise project ID or **all_granted_eps**. If the value is a specific enterprise project ID, only resources in the enterprise project are queried. If the value is **all_granted_eps**, resources in the enterprise projects with the **elb:listeners:list** permission are queried. Multiple values can be queried in the format of *enterprise_project_id=xxx&enterprise_project_id=xxx*.
enable_member_retry	No	Boolean	Specifies whether to enable health check retries for backend servers. The value can be **true** (enable health check retries) or **false** (disable health check retries).

Parameter	Mandatory	Type	Description
member_timeout	No	Array of integers	Specifies the timeout duration for waiting for a response from a backend server, in seconds. If the backend server fails to respond after the timeout duration elapses, the load balancer will stop waiting and return HTTP 504 Gateway Timeout to the client. The value ranges from **1** to **300**. Multiple durations can be queried in the format of *member_timeout=xxx&member_timeout=xxx*.
client_timeout	No	Array of integers	Specifies the timeout duration for waiting for a response from a client, in seconds. There are two situations: • If the client fails to send a request header to the load balancer within the timeout duration, the request will be interrupted. • If the interval between two consecutive request bodies reaching the load balancer is greater than the timeout duration, the connection will be disconnected. The value ranges from **1** to **300**. Multiple durations can be queried in the format of *client_timeout=xxx&client_timeout=xxx*.

Parameter	Mandatory	Type	Description
keepalive_timeout	No	Array of integers	Specifies the idle timeout duration, in seconds. If there are no requests reaching the load balancer after the idle timeout duration elapses, the load balancer will disconnect the connection with the client and establish a new connection when there is a new request. Value ranges: • For TCP listeners, the value ranges from **10** to **4000**. • For HTTP, HTTPS, and TERMINATED_HTTPS listeners, the value ranges from **0** to **4000**. The default value is **60**. Multiple values can be queried in the format of *keepalive_timeout=xxx&keepalive_timeout=xxx*.
transparent_client_ip_enable	No	Boolean	Specifies whether to pass source IP addresses of the clients to backend servers. This parameter is only available for TCP or UDP listeners of shared load balancers. Value options: • **true**: Source IP addresses will be passed to backend servers. • **false**: Source IP addresses will not be passed to backend servers.
proxy_protocol_enable	No	Boolean	Specifies whether to enable the ProxyProtocol option to pass the source IP addresses of the clients to backend servers. This parameter is available only for TLS listeners and does not take effect for other types of listeners.

Parameter	Mandatory	Type	Description
enhance_l7policy_enable	No	Boolean	Specifies whether to enable advanced forwarding. If you enable this function, you can configure more flexible forwarding policies and rules. • **true**: Enable advanced forwarding. • **false**: Disable advanced forwarding.
member_instance_id	No	Array of strings	Specifies the backend server ID. This parameter is used only as a query condition and is not included in the response. Multiple IDs can be queried in the format of *member_instance_id=xxx&member_instance_id=xxx*.
protection_status	No	Array of strings	Specifies the protection status. Value options: • **nonProtection** (default): The load balancer is not protected. • **consoleProtection**: **Modification Protection** is enabled on the console.
ssl_early_data_enable	No	Boolean	Specifies whether to enable zero round trip time resumption (0-RTT) for listeners.
nat64_enable	No	Boolean	Specifies a **nat64_enable** value for query. Resources can be queried in the format of **nat64_enable=true** or **nat64_enable=false**.

Request Parameters

Table 5-301 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-302 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
page_info	**PageInfo** object	Shows pagination information about listeners.
listeners	Array of **Listener** objects	Lists the listeners.

Table 5-303 PageInfo

Parameter	Type	Description
previous_marker	String	Specifies the ID of the first record in the pagination query result. When **page_reverse** is set to **true**, this parameter is used together to query resources on the previous page.
next_marker	String	Specifies the ID of the last record in the pagination query result.
current_count	Integer	Specifies the number of records.

Table 5-304 Listener

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the listener.

Parameter	Type	Description
client_ca_tls_container_ref	String	Specifies the ID of the CA certificate used by the listener. Note: This parameter is available only when **type** is set to **client**.
connection_limit	Integer	Specifies the maximum number of connections that the load balancer can establish with backend servers. **-1** indicates that the number of connections is not limited. Default value: **-1** This parameter is unsupported. Please do not use it.
created_at	String	Specifies the time when the listener was created, in the format of *yyyy-MM-dd''T''HH:mm:ss''Z''*, for example, 2021-07-30T12:03:44Z.
default_pool_id	String	Specifies the ID of the default backend server group. If there is no matched forwarding policy, requests are forwarded to the default backend server.
default_tls_container_ref	String	Specifies the ID of the server certificate used by the listener.
description	String	Provides supplementary information about the listener.
http2_enable	Boolean	Specifies whether to use HTTP/2 if you want the clients to use HTTP/2 to communicate with the load balancer. Request forwarding using HTTP/2 improves the access performance between your application and the load balancer. However, the load balancer still uses HTTP/1.x to forward requests to the backend server. Note: • This parameter is available only for HTTPS listeners. • If you configure this parameter for listeners with other protocols, it will not take effect. • For QUIC listeners, it cannot be set and the response is fixed at **true**.
id	String	Specifies the listener ID.

Parameter	Type	Description
insert_headers	**ListenerInsertHeaders** object	Specifies the HTTP header fields that can transmit required information to backend servers. For example, the X-Forwarded-ELB-IP header field can transmit the EIP of the load balancer to backend servers.
loadbalancers	Array of **LoadBalancerRef** objects	Specifies the ID of the load balancer that the listener is added to. A listener can be added to only one load balancer.
name	String	Specifies the listener name. Note: If you leave the listener name empty, you cannot locate it on the listener list and view its details.
project_id	String	Specifies the ID of the project where the listener is used.
enterprise_project_id	String	Specifies the ID of the enterprise project.
protocol	String	Specifies the protocol used by the listener. The value can be **TCP**, **UDP**, **HTTP**, **HTTPS**, **TERMINATED_HTTPS**, **QUIC**, or **TLS**. Note: • Protocol used by HTTPS listeners added to a shared load balancer can only be set to **TERMINATED_HTTPS**. If **HTTPS** is passed, the value will be automatically changed to **TERMINATED_HTTPS**. • Protocol used by HTTPS listeners added to a dedicated load balancer can only be set to **HTTPS**. If **TERMINATED_HTTPS** is passed, the value will be automatically changed to **HTTPS**.
protocol_port	Integer	Specifies the port used by the listener. Note: • The QUIC listener port cannot be 4789 or the same as the UDP listener port. • If this parameter is set to **0**, **port_ranges** is required.

Parameter	Type	Description
sni_container_refs	Array of strings	Specifies the IDs of SNI certificates (server certificates with domain names) used by the listener. Note: • The domain names of all SNI certificates must be unique. • The total number of domain names of all SNI certificates cannot exceed 50.
sni_match_algo	String	Specifies how wildcard domain name matches with the SNI certificates used by the listener. Value options: • **longest_suffix**: indicates longest suffix match. • **wildcard** (default): indicates wildcard match.
tags	Array of **Tag** objects	Lists the tags.
updated_at	String	Specifies the time when the listener was updated, in the format of *yyyy-MM-dd''T''HH:mm:ss''Z''*, for example, 2021-07-30T12:03:44Z.
tls_ciphers_policy	String	Specifies the security policy used by the listener. The value can be **tls-1-0-inherit**, **tls-1-0**, **tls-1-1**, **tls-1-2** (default), **tls-1-2-strict**, **tls-1-2-fs**, **tls-1-0-with-1-3**, **tls-1-2-fs-with-1-3**, **hybrid-policy-1-0**, or **tls-1-2-strict-no-cbc**. Note: • This parameter will take effect only for HTTPS listeners added to a dedicated load balancer. • This parameter is not available for QUIC listeners. • If both **security_policy_id** and **tls_ciphers_policy** are specified, only **security_policy_id** will take effect. • The encryption suite priority from the highest to lowest is ECC suite, RSA suite, and finally TLS 1.3 suite (supporting both ECC and RSA).

Parameter	Type	Description
security_policy_id	String	Specifies the ID of the custom security policy. Note: • This parameter will take effect only for HTTPS listeners added to a dedicated load balancer. • This parameter is not available for QUIC listeners. • If both **security_policy_id** and **tls_ciphers_policy** are specified, only **security_policy_id** will take effect. • The encryption suite priority from highest to lowest is ECC suite, RSA suite, and finally TLS 1.3 suite (supporting both ECC and RSA).
enable_member_retry	Boolean	Specifies whether to enable health check retries for backend servers. Value options: • **true** (default): Health check retries will be enabled. • **false**: Health check retries will be disabled. Note: • If a shared load balancer is associated, this parameter is available only when **protocol** is set to **HTTP** or **TERMINATED_HTTPS**. • If a dedicated load balancer is associated, this parameter is available only when **protocol** is set to **HTTP**, **HTTPS**, or **QUIC**.

Parameter	Type	Description
keepalive_timeout	Integer	Specifies the idle timeout duration, in seconds. If there are no requests reaching the load balancer after the idle timeout duration elapses, the load balancer will disconnect the connection with the client and establish a new connection when there is a new request. Value ranges: • For TCP listeners, the value ranges from **10** to **4000**, and the default value is **300**. • For HTTP, HTTPS, and TERMINATED_HTTPS listeners, the value ranges from **0** to **4000**, and the default value is **60**. Note: This parameter is not supported by UDP listeners of shared load balancers.
client_timeout	Integer	Specifies the timeout duration for waiting for a response from a client, in seconds. There are two situations: • If the client fails to send a request header to the load balancer within the timeout duration, the request will be interrupted. • If the interval between two consecutive request bodies reaching the load balancer is greater than the timeout duration, the connection will be disconnected. The value ranges from **1** to **300**, and the default value is **60**. This parameter is available only for HTTP and HTTPS listeners.

Parameter	Type	Description
member_timeout	Integer	Specifies the timeout duration for waiting for a response from a backend server, in seconds. If the backend server fails to respond after the timeout duration elapses, the load balancer will stop waiting and return HTTP 504 Gateway Timeout to the client. The value ranges from **1** to **300**, and the default value is **60**. This parameter is available only for HTTP and HTTPS listeners.
ipgroup	**ListenerIpGroup** object	Specifies the IP address group associated with the listener.
transparent_client_ip_enable	Boolean	Specifies whether to pass source IP addresses of the clients to backend servers. Value options: • TCP or UDP listeners of shared load balancers: The value can be **true** or **false**, and the default value is **false** if this parameter is not passed. • HTTP or HTTPS listeners of shared load balancers: The value can only be **true**, and the default value is **true** if this parameter is not passed. • All listeners of dedicated load balancers: The value can only be **true**, and the default value is **true** if this parameter is not passed. Note: • This function can only be enabled or disabled for TCP or UDP listeners of shared load balancers. • If this function is enabled, the load balancer communicates with backend servers using their real IP addresses. Ensure that security group rules and access control policies are correctly configured. • If this function is enabled, a server cannot serve as both a backend server and a client. • If this function is enabled, backend server specifications cannot be changed.

Parameter	Type	Description
proxy_protocol_enable	Boolean	Specifies whether to enable the ProxyProtocol option to pass the source IP addresses of the clients to backend servers. Note: This parameter is available only for TLS listeners and does not take effect for other types of listeners.
enhance_l7policy_enable	Boolean	Specifies whether to enable advanced forwarding. If advanced forwarding is enabled, more flexible forwarding policies and rules are supported. Value options: • **true**: Enable advanced forwarding. • **false** (default): Disable advanced forwarding. The following scenarios are supported: • **action** can be set to **REDIRECT_TO_URL** (requests will be redirected to another URL) or **FIXED_RESPONSE** (a fixed response body will be returned to clients). • Parameters **priority**, **redirect_url_config**, and **fixed_response_config** can be specified in a forwarding policy. • **type** can be set to **METHOD**, **HEADER**, **QUERY_STRING**, or **SOURCE_IP** for a forwarding rule. • If **type** is set to **HOST_NAME** for a forwarding rule, the value of the forwarding rule supports wildcard asterisks (*). • Parameter **conditions** can be specified for forwarding rules. Note: • Advanced forwarding cannot be disabled once it is enabled. • If advanced forwarding is enabled, forwarding policy priorities are defined by **priority**. For details, see the description of the **priority** field in the forwarding policy.

Parameter	Type	Description
quic_config	**ListenerQuicConfig** object	Specifies the QUIC configuration for the current listener. Note: • This parameter is valid only when **protocol** is set to **HTTPS**. For a TCP, UDP, HTTP, or QUIC listener, if this parameter is not left blank, an error will be reported. • The client sends a normal HTTP request that contains information indicating that the QUIC protocol is supported. If QUIC upgrade is enabled for the listeners, QUIC port and version information will be added to the response header. When the client sends both HTTPS and QUIC requests to the server, if the QUIC request is successfully sent, QUIC protocol will be used for subsequent communications.
protection_status	String	Specifies the protection status. Value options: • **nonProtection** (default): The load balancer is not protected. • **consoleProtection**: **Modification Protection** is enabled on the console.
protection_reason	String	Specifies why the modification protection is enabled. Note: This parameter is valid only when **protection_status** is set to **consoleProtection**. The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).
gzip_enable	Boolean	Specifies whether to enable gzip compression for a load balancer. The value can be **true** or **false**, and the default value is **false**. Note: This parameter can be configured only for HTTP, HTTPS, and QUIC listeners.

Parameter	Type	Description
port_ranges	Array of **PortRange** objects	Specifies the port range, including the start and end port numbers. Note: • A maximum of 10 port ranges can be specified. The port range cannot overlap with each other. • This parameter can be specified only when **protocol_port** is set to **0**.
ssl_early_data_enable	Boolean	Specifies whether to enable zero round trip time resumption (0-RTT) for listeners. The default value is **false**. This option can be configured only for HTTPS listeners and depends on the TLS 1.3 security policy protocols.
cps	Integer	Specifies the maximum number of new connections that a listener can handle per second. Value range: **0** to **1000000** Default value: **0**, indicating that the number is not limited. Note: If the value is greater than the number defined in the load balancer specifications, the latter is used as the limit.
connection	Integer	Specifies the maximum number of concurrent connections that a listener can handle per second. Value range: **0** to **1000000** Default value: **0**, indicating that the number is not limited. Note: If the value is greater than the number defined in the load balancer specifications, the latter is used as the limit.

Parameter	Type	Description
nat64_enable	Boolean	Specifies whether to enable **nat64_enable**. This function enables a client to access IPv4 or IPv6 backend servers by accessing the IPv4 or IPv6 address of a load balancer. Constraints: This option can only be enabled for TCP and UDP listeners. **nat64_enable** is mutually exclusive with **transparent_client_ip_enable**. Value options: **true**: Enable **nat64_enable**. **false**: Disable **nat64_enable**. Default value: **false**

Table 5-305 ListenerInsertHeaders

Parameter	Type	Description
X-Forwarded-ELB-IP	Boolean	Specifies whether to transparently transmit the load balancer EIP to backend servers. If **X-Forwarded-ELB-IP** is set to **true**, the load balancer EIP will be stored in the HTTP header and passed to backend servers.
X-Forwarded-Port	Boolean	Specifies whether to transparently transmit the listening port of the load balancer to backend servers. If **X-Forwarded-Port** is set to **true**, the listening port of the load balancer will be stored in the HTTP header and passed to backend servers.
X-Forwarded-For-Port	Boolean	Specifies whether to transparently transmit the source port of the client to backend servers. If **X-Forwarded-For-Port** is set to **true**, the source port of the client will be stored in the HTTP header and passed to backend servers.
X-Forwarded-Host	Boolean	Specifies whether to rewrite the **X-Forwarded-Host** header. If **X-Forwarded-Host** is set to **true**, **X-Forwarded-Host** in the request header from the clients can be set to **Host** in the request header sent from the load balancer to backend servers.

Parameter	Type	Description
X-Forwarded-Proto	Boolean	If **X-Forwarded-Proto** is set to **true**, the listener protocol of the load balancer can be transferred to backend servers through the HTTP header of the packet.
X-Real-IP	Boolean	If **X-Real-IP** is set to **true**, the source IP address of the client can be transferred to backend servers through the HTTP header of the packet.
X-Forwarded-ELB-ID	Boolean	If **X-Forwarded-ELB-ID** is set to **true**, the load balancer ID can be transferred to backend servers through the HTTP header of the packet.
X-Forwarded-TLS-Certificate-ID	Boolean	If **X-Forwarded-TLS-Certificate-ID** is set to **true**, the certificate ID of the load balancer can be transferred to backend servers through the HTTP header of the packet.
X-Forwarded-TLS-Protocol	Boolean	If **X-Forwarded-TLS-Protocol** is set to **true**, the algorithm protocol of the load balancer can be transferred to backend servers through the HTTP header of the packet.
X-Forwarded-TLS-Cipher	Boolean	If **X-Forwarded-TLS-Cipher** is set to **true**, the algorithm suite of the load balancer can be transferred to backend servers through the HTTP header of the packet.

Table 5-306 LoadBalancerRef

Parameter	Type	Description
id	String	Specifies the load balancer ID.

Table 5-307 Tag

Parameter	Type	Description
key	String	Specifies the tag key.
value	String	Specifies the tag value.

Table 5-308 ListenerIpGroup

Parameter	Type	Description
ipgroup_id	String	Specifies the ID of the IP address group associated with the listener. This parameter is mandatory when you create the IP address group and is optional when you update the IP address group. Note: The specified IP address group must exist, and the value cannot be **null**.
enable_ipgroup	Boolean	Specifies whether access control is enabled. Value options: • **true**: Access control is enabled. • **false**: Access control is disabled. A listener with access control enabled can be directly deleted.
type	String	Specifies how access to the listener is controlled. Value options: • **white** (default): A whitelist will be configured. Only IP addresses in the whitelist can access the listener. • **black**: A blacklist will be configured. IP addresses in the blacklist are not allowed to access the listener.

Table 5-309 ListenerQuicConfig

Parameter	Type	Description
quic_listener_id	String	Specifies the ID of the QUIC listener. This parameter is mandatory for creation and is optional for update. The listener specified by **quic_listener_id** must exist. The listener protocol must be **QUIC** and cannot be set to **null**, otherwise, it will conflict with **enable_quic_upgrade**.

Parameter	Type	Description
enable_quic_upgrade	Boolean	Specifies whether to enable QUIC upgrade. Value options: • **true**: QUIC upgrade is enabled. • **false**: QUIC upgrade is disabled. HTTPS listeners can be upgraded to QUIC listeners.

Table 5-310 PortRange

Parameter	Type	Description
start_port	Integer	Specifies the start port number.
end_port	Integer	Specifies the end port number. The value must be greater than or equal to the start port number.

Example Requests

Queries the listeners on each page

```
GET https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/listeners?
limit=2&marker=0r31747a-b139-492f-2749-2df0b1c87193
```

Example Responses

Status code: 200

Successful request.

```
{
  "listeners" : [ {
    "id" : "0b11747a-b139-492f-9692-2df0b1c87193",
    "name" : "My listener",
    "protocol_port" : 80,
    "protocol" : "TCP",
    "ipgroup" : null,
    "description" : "My listener update.",
    "default_tls_container_ref" : null,
    "admin_state_up" : true,
    "loadbalancers" : [ {
      "id" : "098b2f68-af1c-41a9-8efd-69958722af62"
    } ],
    "member_timeout" : null,
    "client_timeout" : null,
    "keepalive_timeout" : 300,
    "client_ca_tls_container_ref" : null,
    "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
    "sni_container_refs" : [ ],
    "connection_limit" : -1,
    "default_pool_id" : null,
    "tls_ciphers_policy" : "tls-1-2",
    "tags" : [ ],
```



```
    "created_at" : "2019-04-02T00:12:32Z",
    "updated_at" : "2019-04-02T17:43:46Z",
    "http2_enable" : true,
    "insert_headers" : {
      "X-Forwarded-ELB-IP" : true
    },
    "transparent_client_ip_enable" : false,
    "quic_config" : null,
    "nat64_enable" : false
  }, {
    "id" : "0b455839-3ea7-4bac-ad26-35bf22f96ea4",
    "name" : "listener-test",
    "protocol_port" : 86,
    "protocol" : "TERMINATED_HTTPS",
    "description" : null,
    "default_tls_container_ref" : "ad9b123e858d4652b80e89b9941e49a4",
    "admin_state_up" : true,
    "loadbalancers" : [ {
      "id" : "309a0f61-0b62-45f2-97d1-742f3434338e"
    } ],
    "member_timeout" : 60,
    "client_timeout" : 60,
    "keepalive_timeout" : 15,
    "client_ca_tls_container_ref" : "7875ccb4c6b44cdb90ab2ab89892ab71",
    "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
    "sni_container_refs" : [ "7f41c96223d34ebaa3c8e836b6625ec0" ],
    "connection_limit" : -1,
    "default_pool_id" : "5e7e0175-d5d5-4f37-bfba-88a9524ad20b",
    "tls_ciphers_policy" : "tls-1-2",
    "tags" : [ ],
    "created_at" : "2019-03-22T23:37:14Z",
    "updated_at" : "2019-03-22T23:37:14Z",
    "http2_enable" : false,
    "ipgroup" : null,
    "insert_headers" : {
      "X-Forwarded-ELB-IP" : true
    },
    "transparent_client_ip_enable" : false,
    "quic_config" : null,
    "nat64_enable" : false
  } ],
  "page_info" : {
    "next_marker" : "0b455839-3ea7-4bac-ad26-35bf22f96ea4",
    "previous_marker" : "0b11747a-b139-492f-9692-2df0b1c87193",
    "current_count" : 2
  },
  "request_id" : "774640ee-6863-4de3-8156-aff16f51a087"
}
```


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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ListListenersSolution {
```

```
    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ListListenersRequest request = new ListListenersRequest();
        try {
            ListListenersResponse response = client.listListeners(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListListenersRequest()
        response = client.list_listeners(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListListenersRequest{}
    response, err := client.ListListeners(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	Successful request.

Error Codes

See **Error Codes**.

5.10.3 Viewing the Details of a Listener

Function

This API is used to view the details of a listener.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/listeners/{listener_id}

Table 5-311 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
listener_id	Yes	String	Specifies the listener ID.

Request Parameters

Table 5-312 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-313 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
listener	**Listener** object	Specifies the listener.

Table 5-314 Listener

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the listener.
client_ca_tls_container_ref	String	Specifies the ID of the CA certificate used by the listener. Note: This parameter is available only when **type** is set to **client**.
connection_limit	Integer	Specifies the maximum number of connections that the load balancer can establish with backend servers. **-1** indicates that the number of connections is not limited. Default value: **-1** This parameter is unsupported. Please do not use it.
created_at	String	Specifies the time when the listener was created, in the format of *yyyy-MM-dd''T''HH:mm:ss''Z''*, for example, 2021-07-30T12:03:44Z.
default_pool_id	String	Specifies the ID of the default backend server group. If there is no matched forwarding policy, requests are forwarded to the default backend server.
default_tls_container_ref	String	Specifies the ID of the server certificate used by the listener.
description	String	Provides supplementary information about the listener.

Parameter	Type	Description
http2_enable	Boolean	Specifies whether to use HTTP/2 if you want the clients to use HTTP/2 to communicate with the load balancer. Request forwarding using HTTP/2 improves the access performance between your application and the load balancer. However, the load balancer still uses HTTP/1.x to forward requests to the backend server. Note: • This parameter is available only for HTTPS listeners. • If you configure this parameter for listeners with other protocols, it will not take effect. • For QUIC listeners, it cannot be set and the response is fixed at **true**.
id	String	Specifies the listener ID.
insert_headers	**ListenerInsertHeaders** object	Specifies the HTTP header fields that can transmit required information to backend servers. For example, the X-Forwarded-ELB-IP header field can transmit the EIP of the load balancer to backend servers.
loadbalancers	Array of **LoadBalancerRef** objects	Specifies the ID of the load balancer that the listener is added to. A listener can be added to only one load balancer.
name	String	Specifies the listener name. Note: If you leave the listener name empty, you cannot locate it on the listener list and view its details.
project_id	String	Specifies the ID of the project where the listener is used.
enterprise_project_id	String	Specifies the ID of the enterprise project.

Parameter	Type	Description
protocol	String	Specifies the protocol used by the listener. The value can be **TCP**, **UDP**, **HTTP**, **HTTPS**, **TERMINATED_HTTPS**, **QUIC**, or **TLS**. Note: • Protocol used by HTTPS listeners added to a shared load balancer can only be set to **TERMINATED_HTTPS**. If **HTTPS** is passed, the value will be automatically changed to **TERMINATED_HTTPS**. • Protocol used by HTTPS listeners added to a dedicated load balancer can only be set to **HTTPS**. If **TERMINATED_HTTPS** is passed, the value will be automatically changed to **HTTPS**.
protocol_port	Integer	Specifies the port used by the listener. Note: • The QUIC listener port cannot be 4789 or the same as the UDP listener port. • If this parameter is set to **0**, **port_ranges** is required.
sni_container_refs	Array of strings	Specifies the IDs of SNI certificates (server certificates with domain names) used by the listener. Note: • The domain names of all SNI certificates must be unique. • The total number of domain names of all SNI certificates cannot exceed 50.
sni_match_algo	String	Specifies how wildcard domain name matches with the SNI certificates used by the listener. Value options: • **longest_suffix**: indicates longest suffix match. • **wildcard** (default): indicates wildcard match.

Parameter	Type	Description
tags	Array of **Tag** objects	Lists the tags.
updated_at	String	Specifies the time when the listener was updated, in the format of *yyyy-MM-dd''T''HH:mm:ss''Z''*, for example, 2021-07-30T12:03:44Z.
tls_ciphers_policy	String	Specifies the security policy used by the listener. The value can be **tls-1-0-inherit**, **tls-1-0**, **tls-1-1**, **tls-1-2** (default), **tls-1-2-strict**, **tls-1-2-fs**, **tls-1-0-with-1-3**, **tls-1-2-fs-with-1-3**, **hybrid-policy-1-0**, or **tls-1-2-strict-no-cbc**. Note: • This parameter will take effect only for HTTPS listeners added to a dedicated load balancer. • This parameter is not available for QUIC listeners. • If both **security_policy_id** and **tls_ciphers_policy** are specified, only **security_policy_id** will take effect. • The encryption suite priority from the highest to lowest is ECC suite, RSA suite, and finally TLS 1.3 suite (supporting both ECC and RSA).
security_policy_id	String	Specifies the ID of the custom security policy. Note: • This parameter will take effect only for HTTPS listeners added to a dedicated load balancer. • This parameter is not available for QUIC listeners. • If both **security_policy_id** and **tls_ciphers_policy** are specified, only **security_policy_id** will take effect. • The encryption suite priority from highest to lowest is ECC suite, RSA suite, and finally TLS 1.3 suite (supporting both ECC and RSA).

Parameter	Type	Description
enable_member_retry	Boolean	Specifies whether to enable health check retries for backend servers. Value options: • **true** (default): Health check retries will be enabled. • **false**: Health check retries will be disabled. Note: • If a shared load balancer is associated, this parameter is available only when **protocol** is set to **HTTP** or **TERMINATED_HTTPS**. • If a dedicated load balancer is associated, this parameter is available only when **protocol** is set to **HTTP**, **HTTPS**, or **QUIC**.
keepalive_timeout	Integer	Specifies the idle timeout duration, in seconds. If there are no requests reaching the load balancer after the idle timeout duration elapses, the load balancer will disconnect the connection with the client and establish a new connection when there is a new request. Value ranges: • For TCP listeners, the value ranges from **10** to **4000**, and the default value is **300**. • For HTTP, HTTPS, and TERMINATED_HTTPS listeners, the value ranges from **0** to **4000**, and the default value is **60**. Note: This parameter is not supported by UDP listeners of shared load balancers.

Parameter	Type	Description
client_timeout	Integer	Specifies the timeout duration for waiting for a response from a client, in seconds. There are two situations: • If the client fails to send a request header to the load balancer within the timeout duration, the request will be interrupted. • If the interval between two consecutive request bodies reaching the load balancer is greater than the timeout duration, the connection will be disconnected. The value ranges from **1** to **300**, and the default value is **60**. This parameter is available only for HTTP and HTTPS listeners.
member_timeout	Integer	Specifies the timeout duration for waiting for a response from a backend server, in seconds. If the backend server fails to respond after the timeout duration elapses, the load balancer will stop waiting and return HTTP 504 Gateway Timeout to the client. The value ranges from **1** to **300**, and the default value is **60**. This parameter is available only for HTTP and HTTPS listeners.
ipgroup	**ListenerIpGroup** object	Specifies the IP address group associated with the listener.

Parameter	Type	Description
transparent_client_ip_enable	Boolean	Specifies whether to pass source IP addresses of the clients to backend servers. Value options: • TCP or UDP listeners of shared load balancers: The value can be **true** or **false**, and the default value is **false** if this parameter is not passed. • HTTP or HTTPS listeners of shared load balancers: The value can only be **true**, and the default value is **true** if this parameter is not passed. • All listeners of dedicated load balancers: The value can only be **true**, and the default value is **true** if this parameter is not passed. Note: • This function can only be enabled or disabled for TCP or UDP listeners of shared load balancers. • If this function is enabled, the load balancer communicates with backend servers using their real IP addresses. Ensure that security group rules and access control policies are correctly configured. • If this function is enabled, a server cannot serve as both a backend server and a client. • If this function is enabled, backend server specifications cannot be changed.
proxy_protocol_enable	Boolean	Specifies whether to enable the ProxyProtocol option to pass the source IP addresses of the clients to backend servers. Note: This parameter is available only for TLS listeners and does not take effect for other types of listeners.

Parameter	Type	Description
enhance_l7policy_enable	Boolean	Specifies whether to enable advanced forwarding. If advanced forwarding is enabled, more flexible forwarding policies and rules are supported. Value options: • **true**: Enable advanced forwarding. • **false** (default): Disable advanced forwarding. The following scenarios are supported: • **action** can be set to **REDIRECT_TO_URL** (requests will be redirected to another URL) or **FIXED_RESPONSE** (a fixed response body will be returned to clients). • Parameters **priority**, **redirect_url_config**, and **fixed_response_config** can be specified in a forwarding policy. • **type** can be set to **METHOD**, **HEADER**, **QUERY_STRING**, or **SOURCE_IP** for a forwarding rule. • If **type** is set to **HOST_NAME** for a forwarding rule, the value of the forwarding rule supports wildcard asterisks (*). • Parameter **conditions** can be specified for forwarding rules. Note: • Advanced forwarding cannot be disabled once it is enabled. • If advanced forwarding is enabled, forwarding policy priorities are defined by **priority**. For details, see the description of the **priority** field in the forwarding policy.

Parameter	Type	Description
quic_config	**ListenerQuicConfig** object	Specifies the QUIC configuration for the current listener. Note: • This parameter is valid only when **protocol** is set to **HTTPS**. For a TCP, UDP, HTTP, or QUIC listener, if this parameter is not left blank, an error will be reported. • The client sends a normal HTTP request that contains information indicating that the QUIC protocol is supported. If QUIC upgrade is enabled for the listeners, QUIC port and version information will be added to the response header. When the client sends both HTTPS and QUIC requests to the server, if the QUIC request is successfully sent, QUIC protocol will be used for subsequent communications.
protection_status	String	Specifies the protection status. Value options: • **nonProtection** (default): The load balancer is not protected. • **consoleProtection**: **Modification Protection** is enabled on the console.
protection_reason	String	Specifies why the modification protection is enabled. Note: This parameter is valid only when **protection_status** is set to **consoleProtection**. The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).
gzip_enable	Boolean	Specifies whether to enable gzip compression for a load balancer. The value can be **true** or **false**, and the default value is **false**. Note: This parameter can be configured only for HTTP, HTTPS, and QUIC listeners.

Parameter	Type	Description
port_ranges	Array of **PortRange** objects	Specifies the port range, including the start and end port numbers. Note: • A maximum of 10 port ranges can be specified. The port range cannot overlap with each other. • This parameter can be specified only when **protocol_port** is set to **0**.
ssl_early_data_enable	Boolean	Specifies whether to enable zero round trip time resumption (0-RTT) for listeners. The default value is **false**. This option can be configured only for HTTPS listeners and depends on the TLS 1.3 security policy protocols.
cps	Integer	Specifies the maximum number of new connections that a listener can handle per second. Value range: **0** to **1000000** Default value: **0**, indicating that the number is not limited. Note: If the value is greater than the number defined in the load balancer specifications, the latter is used as the limit.
connection	Integer	Specifies the maximum number of concurrent connections that a listener can handle per second. Value range: **0** to **1000000** Default value: **0**, indicating that the number is not limited. Note: If the value is greater than the number defined in the load balancer specifications, the latter is used as the limit.

Parameter	Type	Description
nat64_enable	Boolean	Specifies whether to enable **nat64_enable**. This function enables a client to access IPv4 or IPv6 backend servers by accessing the IPv4 or IPv6 address of a load balancer. Constraints: This option can only be enabled for TCP and UDP listeners. **nat64_enable** is mutually exclusive with **transparent_client_ip_enable**. Value options: **true**: Enable **nat64_enable**. **false**: Disable **nat64_enable**. Default value: **false**

Table 5-315 ListenerInsertHeaders

Parameter	Type	Description
X-Forwarded-ELB-IP	Boolean	Specifies whether to transparently transmit the load balancer EIP to backend servers. If **X-Forwarded-ELB-IP** is set to **true**, the load balancer EIP will be stored in the HTTP header and passed to backend servers.
X-Forwarded-Port	Boolean	Specifies whether to transparently transmit the listening port of the load balancer to backend servers. If **X-Forwarded-Port** is set to **true**, the listening port of the load balancer will be stored in the HTTP header and passed to backend servers.
X-Forwarded-For-Port	Boolean	Specifies whether to transparently transmit the source port of the client to backend servers. If **X-Forwarded-For-Port** is set to **true**, the source port of the client will be stored in the HTTP header and passed to backend servers.
X-Forwarded-Host	Boolean	Specifies whether to rewrite the **X-Forwarded-Host** header. If **X-Forwarded-Host** is set to **true**, **X-Forwarded-Host** in the request header from the clients can be set to **Host** in the request header sent from the load balancer to backend servers.

Parameter	Type	Description
X-Forwarded-Proto	Boolean	If **X-Forwarded-Proto** is set to **true**, the listener protocol of the load balancer can be transferred to backend servers through the HTTP header of the packet.
X-Real-IP	Boolean	If **X-Real-IP** is set to **true**, the source IP address of the client can be transferred to backend servers through the HTTP header of the packet.
X-Forwarded-ELB-ID	Boolean	If **X-Forwarded-ELB-ID** is set to **true**, the load balancer ID can be transferred to backend servers through the HTTP header of the packet.
X-Forwarded-TLS-Certificate-ID	Boolean	If **X-Forwarded-TLS-Certificate-ID** is set to **true**, the certificate ID of the load balancer can be transferred to backend servers through the HTTP header of the packet.
X-Forwarded-TLS-Protocol	Boolean	If **X-Forwarded-TLS-Protocol** is set to **true**, the algorithm protocol of the load balancer can be transferred to backend servers through the HTTP header of the packet.
X-Forwarded-TLS-Cipher	Boolean	If **X-Forwarded-TLS-Cipher** is set to **true**, the algorithm suite of the load balancer can be transferred to backend servers through the HTTP header of the packet.

Table 5-316 LoadBalancerRef

Parameter	Type	Description
id	String	Specifies the load balancer ID.

Table 5-317 Tag

Parameter	Type	Description
key	String	Specifies the tag key.
value	String	Specifies the tag value.

Table 5-318 ListenerIpGroup

Parameter	Type	Description
ipgroup_id	String	Specifies the ID of the IP address group associated with the listener. This parameter is mandatory when you create the IP address group and is optional when you update the IP address group. Note: The specified IP address group must exist, and the value cannot be **null**.
enable_ipgroup	Boolean	Specifies whether access control is enabled. Value options: • **true**: Access control is enabled. • **false**: Access control is disabled. A listener with access control enabled can be directly deleted.
type	String	Specifies how access to the listener is controlled. Value options: • **white** (default): A whitelist will be configured. Only IP addresses in the whitelist can access the listener. • **black**: A blacklist will be configured. IP addresses in the blacklist are not allowed to access the listener.

Table 5-319 ListenerQuicConfig

Parameter	Type	Description
quic_listener_id	String	Specifies the ID of the QUIC listener. This parameter is mandatory for creation and is optional for update. The listener specified by **quic_listener_id** must exist. The listener protocol must be **QUIC** and cannot be set to **null**, otherwise, it will conflict with **enable_quic_upgrade**.

Parameter	Type	Description
enable_quic_upgrade	Boolean	Specifies whether to enable QUIC upgrade. Value options: • **true**: QUIC upgrade is enabled. • **false**: QUIC upgrade is disabled. HTTPS listeners can be upgraded to QUIC listeners.

Table 5-320 PortRange

Parameter	Type	Description
start_port	Integer	Specifies the start port number.
end_port	Integer	Specifies the end port number. The value must be greater than or equal to the start port number.

Example Requests

Viewing the details of a listener

```
GET https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/listeners/0b11747a-b139-492f-9692-2df0b1c87193
```

Example Responses

Status code: 200

Successful request.

```
{
  "listener" : {
    "id" : "0b11747a-b139-492f-9692-2df0b1c87193",
    "name" : "My listener",
    "protocol_port" : 80,
    "protocol" : "TCP",
    "ipgroup" : null,
    "description" : "My listener update.",
    "default_tls_container_ref" : null,
    "admin_state_up" : true,
    "loadbalancers" : [ {
      "id" : "098b2f68-af1c-41a9-8efd-69958722af62"
    } ],
    "member_timeout" : null,
    "client_timeout" : null,
    "keepalive_timeout" : 300,
    "client_ca_tls_container_ref" : null,
    "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
    "sni_container_refs" : [ ],
    "connection_limit" : -1,
    "default_pool_id" : null,
    "tls_ciphers_policy" : "tls-1-0",
    "tags" : [ ],
```



```
    "created_at" : "2019-04-02T00:12:32Z",
    "updated_at" : "2019-04-02T17:43:46Z",
    "http2_enable" : true,
    "insert_headers" : {
      "X-Forwarded-ELB-IP" : true
    },
    "transparent_client_ip_enable" : false,
    "nat64_enable" : false
  },
  "request_id" : "1394eb39-e4c8-4177-b96d-aaff569f1833"
}
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ShowListenerSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowListenerRequest request = new ShowListenerRequest();
        request.withListenerId("{listener_id}");
        try {
            ShowListenerResponse response = client.showListener(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowListenerRequest()
        request.listener_id = "{listener_id}"
        response = client.show_listener(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowListenerRequest{}
    request.ListenerId = "{listener_id}"
    response, err := client.ShowListener(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	Successful request.

Error Codes

See **Error Codes**.

5.10.4 Updating a Listener

Function

This API is used to update a listener.

Constraints

If the provisioning status of the load balancer that the listener is added to is not **ACTIVE**, the listener cannot be updated.

Calling Method

For details, see **Calling APIs**.

URI

PUT /v3/{project_id}/elb/listeners/{listener_id}

Table 5-321 Path Parameters

Parameter	Mandatory	Type	Description
listener_id	Yes	String	Specifies the listener ID.
project_id	Yes	String	Specifies the project ID.

Request Parameters

Table 5-322 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Table 5-323 Request body parameters

Parameter	Mandatory	Type	Description
listener	Yes	**UpdateListenerOption** object	Request body for updating a listener

Table 5-324 UpdateListenerOption

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Specifies the administrative status of the listener. The value can only be updated to **true**.
client_ca_tls_container_ref	No	String	Specifies the ID of the CA certificate used by the listener. Note: • This parameter is available only when **type** is set to **client**. • This parameter is not available if the listener protocol is **QUIC**.

Parameter	Mandatory	Type	Description
default_pool_id	No	String	Specifies the ID of the default backend server group. If there is no matched forwarding policy, requests are forwarded to the default backend server.
default_tls_container_ref	No	String	Specifies the ID of the server certificate used by the listener. This parameter is available only when the listener's protocol is HTTPS and **type** is set to **server**.
description	No	String	Provides supplementary information about the listener.
http2_enable	No	Boolean	Specifies whether to use HTTP/2 if you want the clients to use HTTP/2 to communicate with the load balancer. Request forwarding using HTTP/2 improves the access performance between your application and the load balancer. However, the load balancer still uses HTTP/1.x to forward requests to the backend server. Note: • This parameter is available only for HTTPS listeners. • If you configure this parameter for listeners with other protocols, it will not take effect. • For QUIC listeners, it cannot be set and the response is fixed at **true**.
insert_headers	No	**ListenerInsertHeaders** object	Specifies the HTTP header fields that can transmit required information to backend servers. For example, the X-Forwarded-ELB-IP header field can transmit the EIP of the load balancer to backend servers.

Parameter	Mandatory	Type	Description
name	No	String	Specifies the listener name. Note: If you leave the listener name empty, you cannot locate it on the listener list and view its details.
sni_container_refs	No	Array of strings	Specifies the IDs of SNI certificates (server certificates with domain names) used by the listener. Note: • The domain names of all SNI certificates must be unique. • The total number of domain names of all SNI certificates cannot exceed 50.
sni_match_algo	No	String	Specifies how wildcard domain name matches with the SNI certificates used by the listener. Value options: • **longest_suffix**: indicates longest suffix match. • **wildcard** (default): indicates wildcard match.

Parameter	Mandatory	Type	Description
tls_ciphers_policy	No	String	Specifies the security policy used by the listener. The value can be **tls-1-0-inherit**, **tls-1-0**, **tls-1-1**, **tls-1-2** (default), **tls-1-2-strict**, **tls-1-2-fs**, **tls-1-0-with-1-3**, **tls-1-2-fs-with-1-3**, **hybrid-policy-1-0**, or **tls-1-2-strict-no-cbc**. Note: • This parameter will take effect only for HTTPS listeners added to a dedicated load balancer. • This parameter is not available for QUIC listeners. • If both **security_policy_id** and **tls_ciphers_policy** are specified, only **security_policy_id** will take effect. • The encryption suite priority from the highest to lowest is ECC suite, RSA suite, and finally TLS 1.3 suite (supporting both ECC and RSA).

Parameter	Mandatory	Type	Description
security_policy_id	No	String	Specifies the ID of the custom security policy. Note: • This parameter will take effect only for HTTPS listeners added to a dedicated load balancer. • This parameter is not available for QUIC listeners. • If both **security_policy_id** and **tls_ciphers_policy** are specified, only **security_policy_id** will take effect. • The encryption suite priority from highest to lowest is ECC suite, RSA suite, and finally TLS 1.3 suite (supporting both ECC and RSA).
enable_member_retry	No	Boolean	Specifies whether to enable health check retries for backend servers. Value options: • **true** (default): Health check retries will be enabled. • **false**: Health check retries will be disabled. Note: • If a shared load balancer is associated, this parameter is available only when **protocol** is set to **HTTP** or **TERMINATED_HTTPS**. • If a dedicated load balancer is associated, this parameter is available only when **protocol** is set to **HTTP**, **HTTPS**, or **QUIC**.

Parameter	Mandatory	Type	Description
member_timeout	No	Integer	Specifies the timeout duration for waiting for a response from a backend server, in seconds. If the backend server fails to respond after the timeout duration elapses, the load balancer will stop waiting and return HTTP 504 Gateway Timeout to the client. The value ranges from **1** to **300**. This parameter is available only for HTTP and HTTPS listeners.
client_timeout	No	Integer	Specifies the timeout duration for waiting for a response from a client, in seconds. This parameter is available only for HTTP and HTTPS listeners. The value ranges from **1** to **300**, and the default value is **60**.
keepalive_timeout	No	Integer	Specifies the idle timeout duration, in seconds. If there are no requests reaching the load balancer after the idle timeout duration elapses, the load balancer will disconnect the connection with the client and establish a new connection when there is a new request. Value ranges: • For TCP listeners, the value ranges from **10** to **4000**. • For HTTP, HTTPS, and TERMINATED_HTTPS listeners, the value ranges from **0** to **4000**. Default value: **60** Note: This parameter is not supported by UDP listeners of shared load balancers.
ipgroup	No	**UpdateListenerIpGroupOption** object	Specifies the IP address group associated with the listener.

Parameter	Mandatory	Type	Description
transparent_client_ip_enable	No	Boolean	Specifies whether to pass source IP addresses of the clients to backend servers. Value options: • TCP or UDP listeners of shared load balancers: The value can be **true** or **false**, and the default value is **false** if this parameter is not passed. • HTTP or HTTPS listeners of shared load balancers: The value can only be **true**, and the default value is **true** if this parameter is not passed. • All listeners of dedicated load balancers: The value can only be **true**, and the default value is **true** if this parameter is not passed. Note: • This function can only be enabled or disabled for TCP or UDP listeners of shared load balancers. • If this function is enabled, the load balancer communicates with backend servers using their real IP addresses. Ensure that security group rules and access control policies are correctly configured. • If this function is enabled, a server cannot serve as both a backend server and a client. • If this function is enabled, backend server specifications cannot be changed.

Parameter	Mandatory	Type	Description
proxy_protocol_enable	No	Boolean	Specifies whether to enable the ProxyProtocol option to pass the source IP addresses of the clients to backend servers. Note: This parameter is available only for TLS listeners and does not take effect for other types of listeners.

Parameter	Mandatory	Type	Description
enhance_l7policy_enable	No	Boolean	Specifies whether to enable advanced forwarding. If advanced forwarding is enabled, more flexible forwarding policies and rules are supported. Value options: • **true**: Enable advanced forwarding. • **false**: Disable advanced forwarding. The following scenarios are supported: • **action** can be set to **REDIRECT_TO_URL** (requests will be redirected to another URL) or **FIXED_RESPONSE** (a fixed response body will be returned to clients). • Parameters **priority**, **redirect_url_config**, and **fixed_response_config** can be specified in a forwarding policy. • **type** can be set to **METHOD**, **HEADER**, **QUERY_STRING**, or **SOURCE_IP** for a forwarding rule. • If **type** is set to **HOST_NAME** for a forwarding rule, the value of the forwarding rule supports wildcard asterisks (*). • Parameter **conditions** can be specified for forwarding rules. Note: • Advanced forwarding cannot be disabled once it is enabled. • If advanced forwarding is enabled, forwarding policy priorities are defined by

Parameter	Mandatory	Type	Description
			priority. For details, see the description of the **priority** field in the forwarding policy.
quic_config	No	**UpdateListenerQuicConfigOption** object	Specifies the QUIC configuration for the current listener. Note: • This parameter is valid only when **protocol** is set to **HTTPS**. For a TCP, UDP, HTTP, or QUIC listener, if this parameter is not left blank, an error will be reported. • The client sends a normal HTTP request that contains information indicating that the QUIC protocol is supported. If QUIC upgrade is enabled for the listeners, QUIC port and version information will be added to the response header. When the client sends both HTTPS and QUIC requests to the server, if the QUIC request is successfully sent, QUIC protocol will be used for subsequent communications.
protection_status	No	String	Specifies the protection status. Value options: • **nonProtection**: The load balancer is not protected. • **consoleProtection**: **Modification Protection** is enabled on the console.

Parameter	Mandatory	Type	Description
protection_reason	No	String	Specifies why the modification protection is enabled. Note: This parameter is valid only when **protection_status** is set to **consoleProtection**. The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).
gzip_enable	No	Boolean	Specifies whether to enable gzip compression for a load balancer. The value can be **true** or **false**, and the default value is **false**. Note: This parameter can be configured only for HTTP, HTTPS, and QUIC listeners.
ssl_early_data_enable	No	Boolean	Specifies whether to enable zero round trip time resumption (0-RTT) for listeners. The default value is **false**. This option can be configured only for HTTPS listeners and depends on the TLS 1.3 security policy protocols. If **ssl_early_data** is set to **true**, replay attacks may occur. Exercise caution when enabling this option.
cps	No	Integer	Specifies the maximum number of new connections that a listener can handle per second. Value range: **0** to **1000000** Default value: **0**, indicating that the number is not limited. Note: If the value is greater than the number defined in the load balancer specifications, the latter is used as the limit.

Parameter	Mandatory	Type	Description
connection	No	Integer	Specifies the maximum number of concurrent connections that a listener can handle per second. Value range: **0** to **1000000** Default value: **0**, indicating that the number is not limited. Note: If the value is greater than the number defined in the load balancer specifications, the latter is used as the limit.
nat64_enable	No	Boolean	Specifies whether to enable **nat64_enable**. This function enables a client to access IPv4 or IPv6 backend servers by accessing the IPv4 or IPv6 address of a load balancer. Constraints: This option can only be enabled for TCP and UDP listeners. **nat64_enable** is mutually exclusive with **transparent_client_ip_enable**. Value options: **true**: Enable **nat64_enable**. **false**: Disable **nat64_enable**. Default value: **false**

Table 5-325 ListenerInsertHeaders

Parameter	Mandatory	Type	Description
X-Forwarded-ELB-IP	No	Boolean	Specifies whether to transparently transmit the load balancer EIP to backend servers. If **X-Forwarded-ELB-IP** is set to **true**, the load balancer EIP will be stored in the HTTP header and passed to backend servers.

Parameter	Mandatory	Type	Description
X-Forwarded-Port	No	Boolean	Specifies whether to transparently transmit the listening port of the load balancer to backend servers. If **X-Forwarded-Port** is set to **true**, the listening port of the load balancer will be stored in the HTTP header and passed to backend servers.
X-Forwarded-For-Port	No	Boolean	Specifies whether to transparently transmit the source port of the client to backend servers. If **X-Forwarded-For-Port** is set to **true**, the source port of the client will be stored in the HTTP header and passed to backend servers.
X-Forwarded-Host	No	Boolean	Specifies whether to rewrite the **X-Forwarded-Host** header. If **X-Forwarded-Host** is set to **true**, **X-Forwarded-Host** in the request header from the clients can be set to **Host** in the request header sent from the load balancer to backend servers.
X-Forwarded-Proto	No	Boolean	If **X-Forwarded-Proto** is set to **true**, the listener protocol of the load balancer can be transferred to backend servers through the HTTP header of the packet.
X-Real-IP	No	Boolean	If **X-Real-IP** is set to **true**, the source IP address of the client can be transferred to backend servers through the HTTP header of the packet.
X-Forwarded-ELB-ID	No	Boolean	If **X-Forwarded-ELB-ID** is set to **true**, the load balancer ID can be transferred to backend servers through the HTTP header of the packet.

Parameter	Mandatory	Type	Description
X-Forwarded-TLS-Certificate-ID	No	Boolean	If **X-Forwarded-TLS-Certificate-ID** is set to **true**, the certificate ID of the load balancer can be transferred to backend servers through the HTTP header of the packet.
X-Forwarded-TLS-Protocol	No	Boolean	If **X-Forwarded-TLS-Protocol** is set to **true**, the algorithm protocol of the load balancer can be transferred to backend servers through the HTTP header of the packet.
X-Forwarded-TLS-Cipher	No	Boolean	If **X-Forwarded-TLS-Cipher** is set to **true**, the algorithm suite of the load balancer can be transferred to backend servers through the HTTP header of the packet.

Table 5-326 UpdateListenerIpGroupOption

Parameter	Mandatory	Type	Description
ipgroup_id	No	String	Specifies the ID of the IP address group associated with the listener. This parameter is mandatory when you create the IP address group and is optional when you update the IP address group. Note: The specified IP address group must exist, and the value cannot be **null**.
enable_ipgroup	No	Boolean	Specifies whether access control is enabled. Value options: • **true**: Access control is enabled. • **false**: Access control is disabled. A listener with access control enabled can be directly deleted.

Parameter	Mandatory	Type	Description
type	No	String	Specifies how access to the listener is controlled. Value options: • **white** (default): A whitelist will be configured. Only IP addresses in the whitelist can access the listener. • **black**: A blacklist will be configured. IP addresses in the blacklist are not allowed to access the listener.

Table 5-327 UpdateListenerQuicConfigOption

Parameter	Mandatory	Type	Description
quic_listener_id	No	String	Specifies the ID of the QUIC listener. This parameter is mandatory for creation and is optional for update. The listener specified by **quic_listener_id** must exist. The listener protocol must be **QUIC** and cannot be set to **null**, otherwise, it will conflict with **enable_quic_upgrade**.
enable_quic_upgrade	No	Boolean	Specifies whether to enable QUIC upgrade. Value options: • **true**: QUIC upgrade is enabled. • **false**: QUIC upgrade is disabled. HTTPS listeners can be upgraded to QUIC listeners.

Response Parameters

Status code: 200

Table 5-328 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
listener	**Listener** object	Response body for adding a listener

Table 5-329 Listener

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the listener.
client_ca_tls_container_ref	String	Specifies the ID of the CA certificate used by the listener. Note: This parameter is available only when **type** is set to **client**.
connection_limit	Integer	Specifies the maximum number of connections that the load balancer can establish with backend servers. **-1** indicates that the number of connections is not limited. Default value: **-1** This parameter is unsupported. Please do not use it.
created_at	String	Specifies the time when the listener was created, in the format of *yyyy-MM-dd''T''HH:mm:ss''Z''*, for example, 2021-07-30T12:03:44Z.
default_pool_id	String	Specifies the ID of the default backend server group. If there is no matched forwarding policy, requests are forwarded to the default backend server.
default_tls_container_ref	String	Specifies the ID of the server certificate used by the listener.
description	String	Provides supplementary information about the listener.

Parameter	Type	Description
http2_enable	Boolean	Specifies whether to use HTTP/2 if you want the clients to use HTTP/2 to communicate with the load balancer. Request forwarding using HTTP/2 improves the access performance between your application and the load balancer. However, the load balancer still uses HTTP/1.x to forward requests to the backend server. Note: • This parameter is available only for HTTPS listeners. • If you configure this parameter for listeners with other protocols, it will not take effect. • For QUIC listeners, it cannot be set and the response is fixed at **true**.
id	String	Specifies the listener ID.
insert_headers	**ListenerInsertHeaders** object	Specifies the HTTP header fields that can transmit required information to backend servers. For example, the X-Forwarded-ELB-IP header field can transmit the EIP of the load balancer to backend servers.
loadbalancers	Array of **LoadBalancerRef** objects	Specifies the ID of the load balancer that the listener is added to. A listener can be added to only one load balancer.
name	String	Specifies the listener name. Note: If you leave the listener name empty, you cannot locate it on the listener list and view its details.
project_id	String	Specifies the ID of the project where the listener is used.
enterprise_project_id	String	Specifies the ID of the enterprise project.

Parameter	Type	Description
protocol	String	Specifies the protocol used by the listener. The value can be **TCP**, **UDP**, **HTTP**, **HTTPS**, **TERMINATED_HTTPS**, **QUIC**, or **TLS**. Note: ● Protocol used by HTTPS listeners added to a shared load balancer can only be set to **TERMINATED_HTTPS**. If **HTTPS** is passed, the value will be automatically changed to **TERMINATED_HTTPS**. ● Protocol used by HTTPS listeners added to a dedicated load balancer can only be set to **HTTPS**. If **TERMINATED_HTTPS** is passed, the value will be automatically changed to **HTTPS**.
protocol_port	Integer	Specifies the port used by the listener. Note: ● The QUIC listener port cannot be 4789 or the same as the UDP listener port. ● If this parameter is set to **0**, **port_ranges** is required.
sni_container_refs	Array of strings	Specifies the IDs of SNI certificates (server certificates with domain names) used by the listener. Note: ● The domain names of all SNI certificates must be unique. ● The total number of domain names of all SNI certificates cannot exceed 50.
sni_match_algo	String	Specifies how wildcard domain name matches with the SNI certificates used by the listener. Value options: ● **longest_suffix**: indicates longest suffix match. ● **wildcard** (default): indicates wildcard match.

Parameter	Type	Description
tags	Array of **Tag** objects	Lists the tags.
updated_at	String	Specifies the time when the listener was updated, in the format of *yyyy-MM-dd''T''HH:mm:ss''Z''*, for example, 2021-07-30T12:03:44Z.
tls_ciphers_policy	String	Specifies the security policy used by the listener. The value can be **tls-1-0-inherit**, **tls-1-0**, **tls-1-1**, **tls-1-2** (default), **tls-1-2-strict**, **tls-1-2-fs**, **tls-1-0-with-1-3**, **tls-1-2-fs-with-1-3**, **hybrid-policy-1-0**, or **tls-1-2-strict-no-cbc**. Note: • This parameter will take effect only for HTTPS listeners added to a dedicated load balancer. • This parameter is not available for QUIC listeners. • If both **security_policy_id** and **tls_ciphers_policy** are specified, only **security_policy_id** will take effect. • The encryption suite priority from the highest to lowest is ECC suite, RSA suite, and finally TLS 1.3 suite (supporting both ECC and RSA).
security_policy_id	String	Specifies the ID of the custom security policy. Note: • This parameter will take effect only for HTTPS listeners added to a dedicated load balancer. • This parameter is not available for QUIC listeners. • If both **security_policy_id** and **tls_ciphers_policy** are specified, only **security_policy_id** will take effect. • The encryption suite priority from highest to lowest is ECC suite, RSA suite, and finally TLS 1.3 suite (supporting both ECC and RSA).

Parameter	Type	Description
enable_member_retry	Boolean	Specifies whether to enable health check retries for backend servers. Value options: • **true** (default): Health check retries will be enabled. • **false**: Health check retries will be disabled. Note: • If a shared load balancer is associated, this parameter is available only when **protocol** is set to **HTTP** or **TERMINATED_HTTPS**. • If a dedicated load balancer is associated, this parameter is available only when **protocol** is set to **HTTP**, **HTTPS**, or **QUIC**.
keepalive_timeout	Integer	Specifies the idle timeout duration, in seconds. If there are no requests reaching the load balancer after the idle timeout duration elapses, the load balancer will disconnect the connection with the client and establish a new connection when there is a new request. Value ranges: • For TCP listeners, the value ranges from **10** to **4000**, and the default value is **300**. • For HTTP, HTTPS, and TERMINATED_HTTPS listeners, the value ranges from **0** to **4000**, and the default value is **60**. Note: This parameter is not supported by UDP listeners of shared load balancers.

Parameter	Type	Description
client_timeout	Integer	Specifies the timeout duration for waiting for a response from a client, in seconds. There are two situations: • If the client fails to send a request header to the load balancer within the timeout duration, the request will be interrupted. • If the interval between two consecutive request bodies reaching the load balancer is greater than the timeout duration, the connection will be disconnected. The value ranges from **1** to **300**, and the default value is **60**. This parameter is available only for HTTP and HTTPS listeners.
member_timeout	Integer	Specifies the timeout duration for waiting for a response from a backend server, in seconds. If the backend server fails to respond after the timeout duration elapses, the load balancer will stop waiting and return HTTP 504 Gateway Timeout to the client. The value ranges from **1** to **300**, and the default value is **60**. This parameter is available only for HTTP and HTTPS listeners.
ipgroup	**ListenerIpGroup** object	Specifies the IP address group associated with the listener.

Parameter	Type	Description
transparent_client_ip_enable	Boolean	Specifies whether to pass source IP addresses of the clients to backend servers. Value options: • TCP or UDP listeners of shared load balancers: The value can be **true** or **false**, and the default value is **false** if this parameter is not passed. • HTTP or HTTPS listeners of shared load balancers: The value can only be **true**, and the default value is **true** if this parameter is not passed. • All listeners of dedicated load balancers: The value can only be **true**, and the default value is **true** if this parameter is not passed. Note: • This function can only be enabled or disabled for TCP or UDP listeners of shared load balancers. • If this function is enabled, the load balancer communicates with backend servers using their real IP addresses. Ensure that security group rules and access control policies are correctly configured. • If this function is enabled, a server cannot serve as both a backend server and a client. • If this function is enabled, backend server specifications cannot be changed.
proxy_protocol_enable	Boolean	Specifies whether to enable the ProxyProtocol option to pass the source IP addresses of the clients to backend servers. Note: This parameter is available only for TLS listeners and does not take effect for other types of listeners.

Parameter	Type	Description
enhance_l7policy_enable	Boolean	Specifies whether to enable advanced forwarding. If advanced forwarding is enabled, more flexible forwarding policies and rules are supported. Value options: • **true**: Enable advanced forwarding. • **false** (default): Disable advanced forwarding. The following scenarios are supported: • **action** can be set to **REDIRECT_TO_URL** (requests will be redirected to another URL) or **FIXED_RESPONSE** (a fixed response body will be returned to clients). • Parameters **priority**, **redirect_url_config**, and **fixed_response_config** can be specified in a forwarding policy. • **type** can be set to **METHOD**, **HEADER**, **QUERY_STRING**, or **SOURCE_IP** for a forwarding rule. • If **type** is set to **HOST_NAME** for a forwarding rule, the value of the forwarding rule supports wildcard asterisks (*). • Parameter **conditions** can be specified for forwarding rules. Note: • Advanced forwarding cannot be disabled once it is enabled. • If advanced forwarding is enabled, forwarding policy priorities are defined by **priority**. For details, see the description of the **priority** field in the forwarding policy.

Parameter	Type	Description
quic_config	**ListenerQuicConfig** object	Specifies the QUIC configuration for the current listener. Note: • This parameter is valid only when **protocol** is set to **HTTPS**. For a TCP, UDP, HTTP, or QUIC listener, if this parameter is not left blank, an error will be reported. • The client sends a normal HTTP request that contains information indicating that the QUIC protocol is supported. If QUIC upgrade is enabled for the listeners, QUIC port and version information will be added to the response header. When the client sends both HTTPS and QUIC requests to the server, if the QUIC request is successfully sent, QUIC protocol will be used for subsequent communications.
protection_status	String	Specifies the protection status. Value options: • **nonProtection** (default): The load balancer is not protected. • **consoleProtection**: **Modification Protection** is enabled on the console.
protection_reason	String	Specifies why the modification protection is enabled. Note: This parameter is valid only when **protection_status** is set to **consoleProtection**. The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).
gzip_enable	Boolean	Specifies whether to enable gzip compression for a load balancer. The value can be **true** or **false**, and the default value is **false**. Note: This parameter can be configured only for HTTP, HTTPS, and QUIC listeners.

Parameter	Type	Description
port_ranges	Array of **PortRange** objects	Specifies the port range, including the start and end port numbers. Note: • A maximum of 10 port ranges can be specified. The port range cannot overlap with each other. • This parameter can be specified only when **protocol_port** is set to **0**.
ssl_early_data_enable	Boolean	Specifies whether to enable zero round trip time resumption (0-RTT) for listeners. The default value is **false**. This option can be configured only for HTTPS listeners and depends on the TLS 1.3 security policy protocols.
cps	Integer	Specifies the maximum number of new connections that a listener can handle per second. Value range: **0** to **1000000** Default value: **0**, indicating that the number is not limited. Note: If the value is greater than the number defined in the load balancer specifications, the latter is used as the limit.
connection	Integer	Specifies the maximum number of concurrent connections that a listener can handle per second. Value range: **0** to **1000000** Default value: **0**, indicating that the number is not limited. Note: If the value is greater than the number defined in the load balancer specifications, the latter is used as the limit.

Parameter	Type	Description
nat64_enable	Boolean	Specifies whether to enable **nat64_enable**. This function enables a client to access IPv4 or IPv6 backend servers by accessing the IPv4 or IPv6 address of a load balancer. Constraints: This option can only be enabled for TCP and UDP listeners. **nat64_enable** is mutually exclusive with **transparent_client_ip_enable**. Value options: **true**: Enable **nat64_enable**. **false**: Disable **nat64_enable**. Default value: **false**

Table 5-330 ListenerInsertHeaders

Parameter	Type	Description
X-Forwarded-ELB-IP	Boolean	Specifies whether to transparently transmit the load balancer EIP to backend servers. If **X-Forwarded-ELB-IP** is set to **true**, the load balancer EIP will be stored in the HTTP header and passed to backend servers.
X-Forwarded-Port	Boolean	Specifies whether to transparently transmit the listening port of the load balancer to backend servers. If **X-Forwarded-Port** is set to **true**, the listening port of the load balancer will be stored in the HTTP header and passed to backend servers.
X-Forwarded-For-Port	Boolean	Specifies whether to transparently transmit the source port of the client to backend servers. If **X-Forwarded-For-Port** is set to **true**, the source port of the client will be stored in the HTTP header and passed to backend servers.
X-Forwarded-Host	Boolean	Specifies whether to rewrite the **X-Forwarded-Host** header. If **X-Forwarded-Host** is set to **true**, **X-Forwarded-Host** in the request header from the clients can be set to **Host** in the request header sent from the load balancer to backend servers.

Parameter	Type	Description
X-Forwarded-Proto	Boolean	If **X-Forwarded-Proto** is set to **true**, the listener protocol of the load balancer can be transferred to backend servers through the HTTP header of the packet.
X-Real-IP	Boolean	If **X-Real-IP** is set to **true**, the source IP address of the client can be transferred to backend servers through the HTTP header of the packet.
X-Forwarded-ELB-ID	Boolean	If **X-Forwarded-ELB-ID** is set to **true**, the load balancer ID can be transferred to backend servers through the HTTP header of the packet.
X-Forwarded-TLS-Certificate-ID	Boolean	If **X-Forwarded-TLS-Certificate-ID** is set to **true**, the certificate ID of the load balancer can be transferred to backend servers through the HTTP header of the packet.
X-Forwarded-TLS-Protocol	Boolean	If **X-Forwarded-TLS-Protocol** is set to **true**, the algorithm protocol of the load balancer can be transferred to backend servers through the HTTP header of the packet.
X-Forwarded-TLS-Cipher	Boolean	If **X-Forwarded-TLS-Cipher** is set to **true**, the algorithm suite of the load balancer can be transferred to backend servers through the HTTP header of the packet.

Table 5-331 LoadBalancerRef

Parameter	Type	Description
id	String	Specifies the load balancer ID.

Table 5-332 Tag

Parameter	Type	Description
key	String	Specifies the tag key.
value	String	Specifies the tag value.

Table 5-333 ListenerIpGroup

Parameter	Type	Description
ipgroup_id	String	Specifies the ID of the IP address group associated with the listener. This parameter is mandatory when you create the IP address group and is optional when you update the IP address group. Note: The specified IP address group must exist, and the value cannot be **null**.
enable_ipgroup	Boolean	Specifies whether access control is enabled. Value options: • **true**: Access control is enabled. • **false**: Access control is disabled. A listener with access control enabled can be directly deleted.
type	String	Specifies how access to the listener is controlled. Value options: • **white** (default): A whitelist will be configured. Only IP addresses in the whitelist can access the listener. • **black**: A blacklist will be configured. IP addresses in the blacklist are not allowed to access the listener.

Table 5-334 ListenerQuicConfig

Parameter	Type	Description
quic_listener_id	String	Specifies the ID of the QUIC listener. This parameter is mandatory for creation and is optional for update. The listener specified by **quic_listener_id** must exist. The listener protocol must be **QUIC** and cannot be set to **null**, otherwise, it will conflict with **enable_quic_upgrade**.

Parameter	Type	Description
enable_quic_upgrade	Boolean	Specifies whether to enable QUIC upgrade. Value options: • **true**: QUIC upgrade is enabled. • **false**: QUIC upgrade is disabled. HTTPS listeners can be upgraded to QUIC listeners.

Table 5-335 PortRange

Parameter	Type	Description
start_port	Integer	Specifies the start port number.
end_port	Integer	Specifies the end port number. The value must be greater than or equal to the start port number.

Example Requests

Modifying the name and description of a listener and enabling the HTTP/2 option

```
PUT https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/listeners/0b11747a-b139-492f-9692-2df0b1c87193

{
  "listener" : {
    "description" : "My listener update.",
    "name" : "My listener",
    "http2_enable" : true
  }
}
```

Example Responses

Status code: 200

Successful request.

```
{
  "listener" : {
    "id" : "0b11747a-b139-492f-9692-2df0b1c87193",
    "name" : "My listener",
    "protocol_port" : 80,
    "protocol" : "TCP",
    "description" : "My listener update.",
    "default_tls_container_ref" : null,
    "admin_state_up" : true,
    "loadbalancers" : [ {
      "id" : "098b2f68-af1c-41a9-8efd-69958722af62"
    } ],
    "member_timeout" : null,
    "client_timeout" : null,
    "keepalive_timeout" : 300,
```



```
  "client_ca_tls_container_ref" : null,
  "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
  "sni_container_refs" : [ ],
  "connection_limit" : -1,
  "default_pool_id" : null,
  "tls_ciphers_policy" : "tls-1-2",
  "tags" : [ ],
  "created_at" : "2019-04-02T00:12:32Z",
  "updated_at" : "2019-04-02T17:43:46Z",
  "http2_enable" : true,
  "ipgroup" : null,
  "insert_headers" : {
    "X-Forwarded-ELB-IP" : true
  },
  "transparent_client_ip_enable" : false,
  "nat64_enable" : false
 },
 "request_id" : "5d56d89a-2271-4a75-8c02-804e3bc7b671"
}
```


SDK Sample Code

The SDK sample code is as follows.

Java

Modifying the name and description of a listener and enabling the HTTP/2 option

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class UpdateListenerSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdateListenerRequest request = new UpdateListenerRequest();
        request.withListenerId("{listener_id}");
        UpdateListenerRequestBody body = new UpdateListenerRequestBody();
        UpdateListenerOption listenerbody = new UpdateListenerOption();
        listenerbody.withDescription("My listener update.")
            .withHttp2Enable(true)
```



```
            .withName("My listener");
        body.withListener(listenerbody);
        request.withBody(body);
        try {
            UpdateListenerResponse response = client.updateListener(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

Modifying the name and description of a listener and enabling the HTTP/2 option

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdateListenerRequest()
        request.listener_id = "{listener_id}"
        listenerbody = UpdateListenerOption(
            description="My listener update.",
            http2_enable=True,
            name="My listener"
        )
        request.body = UpdateListenerRequestBody(
            listener=listenerbody
        )
        response = client.update_listener(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

Modifying the name and description of a listener and enabling the HTTP/2 option

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdateListenerRequest{}
    request.ListenerId = "{listener_id}"
    descriptionListener:= "My listener update."
    http2EnableListener:= true
    nameListener:= "My listener"
    listenerbody := &model.UpdateListenerOption{
        Description: &descriptionListener,
        Http2Enable: &http2EnableListener,
        Name: &nameListener,
    }
    request.Body = &model.UpdateListenerRequestBody{
        Listener: listenerbody,
    }
    response, err := client.UpdateListener(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	Successful request.

Error Codes

See **Error Codes**.

5.10.5 Deleting a Listener

Function

This API is used to delete a listener.

Constraints

Before you delete a listener, delete associated backend server groups or remove all backend servers in the default backend server group, and delete all forwarding policies.

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v3/{project_id}/elb/listeners/{listener_id}

Table 5-336 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
listener_id	Yes	String	Specifies the listener ID.

Request Parameters

Table 5-337 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

None

Example Requests

Deleting a listener

```
DELETE https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/listeners/0b11747a-b139-492f-9692-2df0b1c87193
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class DeleteListenerSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteListenerRequest request = new DeleteListenerRequest();
        request.withListenerId("{listener_id}");
        try {
            DeleteListenerResponse response = client.deleteListener(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteListenerRequest()
        request.listener_id = "{listener_id}"
        response = client.delete_listener(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteListenerRequest{}
    request.ListenerId = "{listener_id}"
    response, err := client.DeleteListener(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	Successful request.

Error Codes

See **Error Codes**.

5.10.6 Deleting a Listener and Its Associated Resources

Function

This API is used to delete a listener and its associated resources, including the forwarding policies and backend server groups.

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v3/{project_id}/elb/listeners/{listener_id}/force

Table 5-338 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
listener_id	Yes	String	Specifies the listener ID.

Request Parameters

Table 5-339 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

None

Example Requests

Deleting a listener and its associated resources

```
DELETE https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/listeners/0b11747a-b139-492f-9692-2df0b1c87193/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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class DeleteListenerForceSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteListenerForceRequest request = new DeleteListenerForceRequest();
        request.withListenerId("{listener_id}");
        try {
            DeleteListenerForceResponse response = client.deleteListenerForce(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteListenerForceRequest()
        request.listener_id = "{listener_id}"
        response = client.delete_listener_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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteListenerForceRequest{}
    request.ListenerId = "{listener_id}"
    response, err := client.DeleteListenerForce(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 DELETE requests.

Error Codes

See **Error Codes**.

5.11 Backend Server Group

5.11.1 Creating a Backend Server Group

Function

This API is used to create a backend server group.

Constraints

Note the following when you create a backend server group:

- If **session-persistence** is specified, **cookie_name** is available only when **type** is set to **APP_COOKIE**.
- If **listener_id** is specified, the listener must have no backend server group associated.

Calling Method

For details, see **Calling APIs**.

URI

POST /v3/{project_id}/elb/pools

Table 5-340 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Request Parameters

Table 5-341 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Table 5-342 Request body parameters

Parameter	Mandatory	Type	Description
pool	Yes	**CreatePoolOption** object	Specifies the request body for creating a backend server group.

Table 5-343 CreatePoolOption

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Specifies the administrative status of the backend server group. The value can only be **true**.
description	No	String	Provides supplementary information about the backend server group.
lb_algorithm	Yes	String	Specifies the load balancing algorithm used by the load balancer to route requests to backend servers in the associated backend server group. Value options: • **ROUND_ROBIN**: weighted round robin • **LEAST_CONNECTIONS**: weighted least connections • **SOURCE_IP**: source IP hash • **QUIC_CID**: connection ID
listener_id	No	String	Specifies the ID of the listener with which the backend server group is associated. Note: • At least one of **listener_id**, **loadbalancer_id**, or **type** must be specified. • Either **listener_id** or **loadbalancer_id** must be specified for shared load balancers. **listener_id** and **loadbalancer_id** are not required for dedicated load balancers.

Parameter	Mandatory	Type	Description
loadbalancer_id	No	String	Specifies the ID of the load balancer with which the backend server group is associated. Note: • Specify one of **listener_id**, **loadbalancer_id**, or **type**, or all of them. • Specify either **listener_id** or **loadbalancer_id** for backend server groups of shared load balancers. **listener_id** and **loadbalancer_id** are not required for backend server groups of dedicated load balancers.
name	No	String	Specifies the backend server group name.
project_id	No	String	Specifies the project ID of the backend server group.

Parameter	Mandatory	Type	Description
protocol	Yes	String	Specifies the protocol used by the backend server group to receive requests. The value can be **TCP**, **UDP**, **TLS**, **HTTP**, **HTTPS**, **GRPC**, or **QUIC**. Note: • If the listener's protocol is **UDP**, the protocol of the backend server group must be **UDP** or **QUIC**. • If the listener's protocol is **TCP**, the protocol of the backend server group must be **TCP**. • If the listener's protocol is **HTTP**, the protocol of the backend server group must be **HTTP**. • If the listener's protocol is **HTTPS**, the protocol of the backend server group can be **HTTP**, **HTTPS**, or **GRPC**. • If the listener's protocol is **TERMINATED_HTTPS**, the protocol of the backend server group must be **HTTP**. • If the listener's protocol is **QUIC**, the protocol of the backend server group can be **HTTP**, **HTTPS**, or **GRPC**. • If the listener's protocol is **TLS**, the protocol of the backend server group can be **TLS** or **TCP**. If protocol of the backend server group is TCP, the **ip_version** must be set to **v4**. Note: • If protocol of the backend server group is QUIC, **session_persistence** must be set to **true**, with **type** set to **SOURCE_IP**. • If protocol of the backend server group is GRPC,

Parameter	Mandatory	Type	Description
			http2_enable of the listener must be set to **true**.
session_persistence	No	**CreatePoolSessionPersistenceOption** object	Specifies the sticky session.
slow_start	No	**CreatePoolSlowStartOption** object	Specifies slow start details. After you enable slow start, new backend servers added to the backend server group are warmed up, and the number of requests they can receive increases linearly during the configured slow start duration. Note: This parameter can be used when the protocol of the backend server group is HTTP or HTTPS.
member_deletion_protection_enable	No	Boolean	Specifies whether to enable deletion protection. Value options: • **true**: Enable deletion protection. • **false** (default): Disable deletion protection. **NOTE** Disable deletion protection for all your resources before deleting your account.

Parameter	Mandatory	Type	Description
vpc_id	No	String	Specifies the ID of the VPC where the backend server group works. Note: • The backend server group must be associated with the VPC. • Only backend servers in the VPC or IP as backend servers can be added. • **type** must be set to **instance**. • If **vpc_id** is not specified, **vpc_id** is determined by the VPC where the backend server works.
type	No	String	Specifies the type of the backend server group. Value options: • **instance**: Any type of backend servers can be added. **vpc_id** is mandatory. • **ip**: Only IP as backend servers can be added. **vpc_id** cannot be specified. Note: • If this parameter is not passed, any type of backend servers can be added. **type** will be returned as an empty string. • Specify one of **listener_id**, **loadbalancer_id**, or **type**. For backend server groups of shared load balancers, specify **loadbalancer_id** or **listener_id**.

Parameter	Mandatory	Type	Description
ip_version	No	String	Specifies the IP address version supported by the backend server group. • Shared load balancers: The value is fixed at **v4**. • Dedicated load balancers: The value can be **dualstack** or **v4**. If the protocol of the backend server group is TCP or UDP, the value is **dualstack**. If the protocol of the backend server group is HTTP, the value is **v4**.
protection_status	No	String	Specifies the protection status. Value options: • **nonProtection** (default): The load balancer is not protected. • **consoleProtection**: **Modification Protection** is enabled on the console.
protection_reason	No	String	Specifies why the modification protection is enabled. Note: This parameter is valid only when **protection_status** is set to **consoleProtection**. The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).

Parameter	Mandatory	Type	Description
any_port_enable	No	Boolean	Specifies whether to enable **any_port_enable** for a backend server group. If this option is enabled, the listener routes the requests to the backend server over the same port as the frontend port. If this option is disabled, the listener routes the requests over the port specified by **protocol_port**. Value options: • **false**: Disable this option. • **true**: Enable this option. Note: This option is available only for TCP, UDP, or QUIC backend server groups.
connection_drain	No	**ConnectionDrain** object	Specifies the configurations of deregistration delay. This parameter is only available for TCP, UDP, and QUIC backend server groups and TCP and UDP listeners. This parameter takes effect when: • A backend server is removed from a backend server group. • A backend server is detected unhealthy or health checks fail. • The weight of a backend server is 0.
pool_health	No	**PoolHealth** object	Specifies the configurations of the pool health feature.
public_border_group	No	String	Specifies the public border group, for example, **center**.
quic_cid_hash_strategy	No	**QuicCidHashStrategy** object	Specifies multi-path forwarding configuration based on destination connection IDs.

Table 5-344 CreatePoolSessionPersistenceOption

Parameter	Mandatory	Type	Description
cookie_name	No	String	Specifies the cookie name. Note: • This parameter will take effect only when **type** is set to **APP_COOKIE**. Otherwise, an error will be returned. Value ranges: • For shared load balancers, the name can contain a maximum of 64 characters, including letters, digits, underscores (_), and hyphens (-). • For dedicated load balancers, the name can contain a maximum of 255 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
type	Yes	String	Specifies the sticky session type. The value can be **SOURCE_IP**, **HTTP_COOKIE**, or **APP_COOKIE**. Note: • If the protocol of the backend server group is **TCP** or **UDP**, only **SOURCE_IP** takes effect. • If the protocol of the backend server group is **HTTP** or **HTTPS**, the value can be **HTTP_COOKIE** or **APP_COOKIE**. • If the backend server group protocol is **QUIC**, sticky session must be enabled with **type** set to **SOURCE_IP**.

Parameter	Mandatory	Type	Description
persistence_timeout	No	Integer	Specifies the stickiness duration, in minutes. This parameter will not take effect when **type** is set to **APP_COOKIE**. Value ranges: • If the protocol of the backend server group is TCP or UDP, the value ranges from **1** to **60**, and the default value is **1**. • If the protocol of the backend server group is HTTP or HTTPS, the value ranges from **1** to **1440**, and the default value is **1440**.

Table 5-345 CreatePoolSlowStartOption

Parameter	Mandatory	Type	Description
enable	No	Boolean	Specifies whether to enable slow start. • **true**: Enable slow start. • **false** (default): Disable slow start.
duration	No	Integer	Specifies the slow start duration, in seconds. The value ranges from **30** to **1200**, and the default value is **30**.

Table 5-346 ConnectionDrain

Parameter	Mandatory	Type	Description
enable	No	Boolean	Specifies whether to enable **connection_drain**. Value options: • **true**: Enable this option. • **false**: Disable this option. Default value: **true**

Parameter	Mandatory	Type	Description
timeout	No	Integer	Specifies the deregistration delay timeout, in seconds. The value ranges from **10** to **4000**.

Table 5-347 PoolHealth

Parameter	Mandatory	Type	Description
minimum_healthy_member_count	No	Integer	If the number of healthy backend servers is less than the value specified for this parameter, the backend server group is considered as unhealthy. The value can be **0** (disabled) or **1** (enabled).

Table 5-348 QuicCidHashStrategy

Parameter	Mandatory	Type	Description
len	Yes	Integer	Specifies the length of the hash factor in the connection ID, in byte. This parameter is valid only when the load balancing algorithm is **QUIC_CID**. Value range: 1 to 20 Default value: 3
offset	Yes	Integer	Specifies the start position in the connection ID as the hash factor, in byte. This parameter is valid only when the load balancing algorithm is **QUIC_CID**. Value range: 0 to 19 Default value: 1

Response Parameters

Status code: 201

Table 5-349 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
pool	**Pool** object	Specifies the backend server group.

Table 5-350 Pool

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the backend server group.
description	String	Provides supplementary information about the backend server group.
healthmonitor_id	String	Specifies the ID of the health check configured for the backend server group.
id	String	Specifies the backend server group ID.
lb_algorithm	String	Specifies the load balancing algorithm used by the load balancer to route requests to backend servers in the associated backend server group. Value options: • **ROUND_ROBIN**: weighted round robin • **LEAST_CONNECTIONS**: weighted least connections • **SOURCE_IP**: source IP hash • **QUIC_CID**: connection ID
listeners	Array of **ListenerRef** objects	Specifies the IDs of the listeners with which the backend server group is associated.
loadbalancers	Array of **LoadBalancerRef** objects	Specifies the IDs of the load balancers with which the backend server group is associated.
members	Array of **MemberRef** objects	Specifies the IDs of the backend servers in the backend server group.
name	String	Specifies the backend server group name.

Parameter	Type	Description
project_id	String	Specifies the project ID.
protocol	String	Specifies the protocol used by the backend server group to receive requests. The value can be **TCP**, **UDP**, **TLS**, **HTTP**, **HTTPS**, **GRPC**, or **QUIC**. Note: • If the listener's protocol is **UDP**, the protocol of the backend server group must be **UDP** or **QUIC**. • If the listener's protocol is **TCP**, the protocol of the backend server group must be **TCP**. • If the listener's protocol is **HTTP**, the protocol of the backend server group must be **HTTP**. • If the listener's protocol is **HTTPS**, the protocol of the backend server group can be **HTTP**, **HTTPS**, or **GRPC**. • If the listener's protocol is **TERMINATED_HTTPS**, the protocol of the backend server group must be **HTTP**. • If the listener's protocol is **QUIC**, the protocol of the backend server group can be **HTTP**, **HTTPS**, or **GRPC**. • If the listener's protocol is **TLS**, the protocol of the backend server group can be **TLS** or **TCP**. If protocol of the backend server group is TCP, the **ip_version** must be set to **v4**. Note: • If protocol of the backend server group is QUIC, **session_persistence** must be set to **true**, with **type** set to **SOURCE_IP**. • If protocol of the backend server group is GRPC, **http2_enable** of the listener must be set to **true**.
session_persistence	**SessionPersistence** object	Specifies the sticky session.

Parameter	Type	Description
ip_version	String	Specifies the IP address version supported by the backend server group. Value range: • Shared load balancers: The value is fixed at **v4**. • Dedicated load balancers: The value can be **dualstack** or **v4**. If the protocol of the backend server group is TCP or UDP, the value is **dualstack**. If the protocol of the backend server group is HTTP, the value is **v4**.
slow_start	**SlowStart** object	Specifies slow start details. After you enable slow start, new backend servers added to the backend server group are warmed up, and the number of requests they can receive increases linearly during the configured slow start duration. This parameter can be used when the protocol of the backend server group is HTTP or HTTPS. An error will be returned if the protocol is not HTTP or HTTPS.
member_deletion_protection_enable	Boolean	Specifies whether to enable deletion protection. Value options: • **true**: Enable deletion protection. • **false**: Disable deletion protection. **NOTE** Disable deletion protection for all your resources before deleting your account.
created_at	String	Specifies the time when the backend server group was created. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.

Parameter	Type	Description
updated_at	String	Specifies the time when the backend server group was updated. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
vpc_id	String	Specifies the ID of the VPC where the backend server group works.
type	String	Specifies the type of the backend server group. Value options: ● **instance**: Any type of backend servers can be added. **vpc_id** is mandatory. ● **ip**: Only IP as backend servers can be added. **vpc_id** cannot be specified. ● **""**: Any type of backend servers can be added.
protection_status	String	Specifies the protection status. Value options: ● **nonProtection** (default): The load balancer is not protected. ● **consoleProtection**: **Modification Protection** is enabled on the console.
protection_reason	String	Specifies why the modification protection is enabled. Note: This parameter is valid only when **protection_status** is set to **consoleProtection**. The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).

Parameter	Type	Description
any_port_enable	Boolean	Specifies whether to enable **any_port_enable** for a backend server group. If this option is enabled, the listener routes the requests to the backend server over the same port as the frontend port. If this option is disabled, the listener routes the requests over the port specified by **protocol_port**. Value options: • **false**: Disable this option. • **true**: Enable this option. Note: This option is available only for TCP, UDP, or QUIC backend server groups.
connection_drain	**ConnectionDrain** object	Specifies the configurations of deregistration delay. This parameter is only available for TCP, UDP, and QUIC backend server groups and TCP and UDP listeners. This parameter takes effect when: • A backend server is removed from a backend server group. • A backend server is detected unhealthy or health checks fail. • The weight of a backend server is 0.
enterprise_project_id	String	Specifies the ID of the enterprise project that the IP address group belongs to.
pool_health	**PoolHealth** object	Specifies the configurations of the pool health feature.
public_border_group	String	Specifies the public border group, for example, **center**.
quic_cid_hash_strategy	**QuicCidHashStrategy** object	Specifies multi-path forwarding policy based on destination connection IDs.

Table 5-351 ListenerRef

Parameter	Type	Description
id	String	Specifies the listener ID.

Table 5-352 LoadBalancerRef

Parameter	Type	Description
id	String	Specifies the load balancer ID.

Table 5-353 MemberRef

Parameter	Type	Description
id	String	Specifies the backend server ID.

Table 5-354 SessionPersistence

Parameter	Type	Description
cookie_name	String	Specifies the cookie name. Note: • This parameter will take effect only when **type** is set to **APP_COOKIE**. Otherwise, an error will be returned. Value ranges: • For shared load balancers, the name can contain a maximum of 64 characters, including letters, digits, underscores (_), and hyphens (-). • For dedicated load balancers, the name can contain a maximum of 255 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).

Parameter	Type	Description
type	String	Specifies the sticky session type. The value can be **SOURCE_IP**, **HTTP_COOKIE**, or **APP_COOKIE**. Note: • If the protocol of the backend server group is **TCP** or **UDP**, only **SOURCE_IP** takes effect. • If the protocol of the backend server group is **HTTP** or **HTTPS**, the value can be **HTTP_COOKIE** or **APP_COOKIE**. • If the backend server group protocol is **QUIC**, sticky session must be enabled with **type** set to **SOURCE_IP**.
persistence_timeout	Integer	Specifies the stickiness duration, in minutes. This parameter will not take effect when **type** is set to **APP_COOKIE**. • If the protocol of the backend server group is TCP, UDP, or QUIC, the value ranges from **1** to **60**, and the default value is **1**. • If the protocol of the backend server group is HTTP or HTTPS, the value ranges from **1** to **1440**, and the default value is **1440**.

Table 5-355 SlowStart

Parameter	Type	Description
enable	Boolean	Specifies whether to enable slow start. • **true**: Enable slow start. • **false** (default): Disable slow start.
duration	Integer	Specifies the slow start duration, in seconds. The value ranges from **30** to **1200**, and the default value is **30**.

Table 5-356 ConnectionDrain

Parameter	Type	Description
enable	Boolean	Specifies whether to enable **connection_drain**. Value options: • **true**: Enable this option. • **false**: Disable this option. Default value: **true**
timeout	Integer	Specifies the deregistration delay timeout, in seconds. The value ranges from **10** to **4000**.

Table 5-357 PoolHealth

Parameter	Type	Description
minimum_healthy_member_count	Integer	If the number of healthy backend servers is less than the value specified for this parameter, the backend server group is considered as unhealthy. The value can be **0** (disabled) or **1** (enabled).

Table 5-358 QuicCidHashStrategy

Parameter	Type	Description
len	Integer	Specifies the length of the hash factor in the connection ID, in byte. This parameter is valid only when the load balancing algorithm is **QUIC_CID**. Value range: 1 to 20 Default value: 3
offset	Integer	Specifies the start position in the connection ID as the hash factor, in byte. This parameter is valid only when the load balancing algorithm is **QUIC_CID**. Value range: 0 to 19 Default value: 1

Example Requests

- Creating a backend server group and setting its backend protocol to TCP

```
POST https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/pools

{
  "pool" : {
    "name" : "My pool",
    "lb_algorithm" : "LEAST_CONNECTIONS",
    "listener_id" : "0b11747a-b139-492f-9692-2df0b1c87193",
    "protocol" : "TCP",
    "member_deletion_protection_enable" : false
  }
}
```

- Creating a backend server group and setting its backend protocol to HTTP

```
POST https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/pools

{
  "pool" : {
    "name" : "My pool",
    "lb_algorithm" : "LEAST_CONNECTIONS",
    "listener_id" : "0b11747a-b139-492f-9692-2df0b1c87193",
    "protocol" : "HTTP",
    "slow_start" : {
      "enable" : true,
      "duration" : 50
    },
    "member_deletion_protection_enable" : false
  }
}
```

Example Responses

Status code: 201

Normal response to POST requests.

```
{
  "pool" : {
    "type" : "",
    "vpc_id" : "",
    "lb_algorithm" : "LEAST_CONNECTIONS",
    "protocol" : "TCP",
    "description" : "",
    "admin_state_up" : true,
    "member_deletion_protection_enable" : false,
    "loadbalancers" : [ {
      "id" : "098b2f68-af1c-41a9-8efd-69958722af62"
    } ],
    "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
    "session_persistence" : null,
    "healthmonitor_id" : null,
    "listeners" : [ {
      "id" : "0b11747a-b139-492f-9692-2df0b1c87193"
    } ],
    "members" : [ ],
    "id" : "36ce7086-a496-4666-9064-5ba0e6840c75",
    "name" : "My pool",
    "ip_version" : "v4",
    "slow_start" : null
  },
  "request_id" : "2d974978-0733-404d-a21a-b29204f4803a"
}
```


SDK Sample Code

The SDK sample code is as follows.

Java

- Creating a backend server group and setting its backend protocol to TCP

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class CreatePoolSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        CreatePoolRequest request = new CreatePoolRequest();
        CreatePoolRequestBody body = new CreatePoolRequestBody();
        CreatePoolOption poolbody = new CreatePoolOption();
        poolbody.withLbAlgorithm("LEAST_CONNECTIONS")
            .withListenerId("0b11747a-b139-492f-9692-2df0b1c87193")
            .withName("My pool")
            .withProtocol("TCP")
            .withMemberDeletionProtectionEnable(false);
        body.withPool(poolbody);
        request.withBody(body);
        try {
            CreatePoolResponse response = client.createPool(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());
        }
    }
}
```


- Creating a backend server group and setting its backend protocol to HTTP

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class CreatePoolSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        CreatePoolRequest request = new CreatePoolRequest();
        CreatePoolRequestBody body = new CreatePoolRequestBody();
        CreatePoolSlowStartOption slowStartPool = new CreatePoolSlowStartOption();
        slowStartPool.withEnable(true)
            .withDuration(50);
        CreatePoolOption poolbody = new CreatePoolOption();
        poolbody.withLbAlgorithm("LEAST_CONNECTIONS")
            .withListenerId("0b11747a-b139-492f-9692-2df0b1c87193")
            .withName("My pool")
            .withProtocol("HTTP")
            .withSlowStart(slowStartPool)
            .withMemberDeletionProtectionEnable(false);
        body.withPool(poolbody);
        request.withBody(body);
        try {
            CreatePoolResponse response = client.createPool(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

- Creating a backend server group and setting its backend protocol to TCP

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreatePoolRequest()
        poolbody = CreatePoolOption(
            lb_algorithm="LEAST_CONNECTIONS",
            listener_id="0b11747a-b139-492f-9692-2df0b1c87193",
            name="My pool",
            protocol="TCP",
            member_deletion_protection_enable=False
        )
        request.body = CreatePoolRequestBody(
            pool=poolbody
        )
        response = client.create_pool(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

- Creating a backend server group and setting its backend protocol to HTTP

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreatePoolRequest()
        slowStartPool = CreatePoolSlowStartOption(
            enable=True,
            duration=50
        )
        poolbody = CreatePoolOption(
            lb_algorithm="LEAST_CONNECTIONS",
            listener_id="0b11747a-b139-492f-9692-2df0b1c87193",
            name="My pool",
            protocol="HTTP",
            slow_start=slowStartPool,
            member_deletion_protection_enable=False
        )
        request.body = CreatePoolRequestBody(
            pool=poolbody
        )
        response = client.create_pool(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

- Creating a backend server group and setting its backend protocol to TCP

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreatePoolRequest{}
```



```
    listenerIdPool:= "0b11747a-b139-492f-9692-2df0b1c87193"
    namePool:= "My pool"
    memberDeletionProtectionEnablePool:= false
    poolbody := &model.CreatePoolOption{
        LbAlgorithm: "LEAST_CONNECTIONS",
        ListenerId: &listenerIdPool,
        Name: &namePool,
        Protocol: "TCP",
        MemberDeletionProtectionEnable: &memberDeletionProtectionEnablePool,
    }
    request.Body = &model.CreatePoolRequestBody{
        Pool: poolbody,
    }
    response, err := client.CreatePool(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

- Creating a backend server group and setting its backend protocol to HTTP

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreatePoolRequest{}
    enableSlowStart:= true
    durationSlowStart:= int32(50)
    slowStartPool := &model.CreatePoolSlowStartOption{
        Enable: &enableSlowStart,
        Duration: &durationSlowStart,
    }
    listenerIdPool:= "0b11747a-b139-492f-9692-2df0b1c87193"
    namePool:= "My pool"
    memberDeletionProtectionEnablePool:= false
    poolbody := &model.CreatePoolOption{
        LbAlgorithm: "LEAST_CONNECTIONS",
        ListenerId: &listenerIdPool,
        Name: &namePool,
        Protocol: "HTTP",
```



```
        SlowStart: slowStartPool,
        MemberDeletionProtectionEnable: &memberDeletionProtectionEnablePool,
    }
    request.Body = &model.CreatePoolRequestBody{
        Pool: poolbody,
    }
    response, err := client.CreatePool(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 POST requests.

Error Codes

See **Error Codes**.

5.11.2 Querying Backend Server Groups

Function

This API is used to query all backend server groups.

Constraints

This API has the following constraints:

- Parameters **marker**, **limit**, and **page_reverse** are used for pagination query.
- Parameters **marker** and **page_reverse** take effect only when they are used together with parameter **limit**.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/pools

Table 5-359 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Table 5-360 Query Parameters

Parameter	Mandatory	Type	Description
marker	No	String	Specifies the ID of the last record on the previous page. Note: • This parameter must be used together with **limit**. • If this parameter is not specified, the first page will be queried. • This parameter cannot be left blank or set to an invalid ID.
limit	No	Integer	Specifies the number of records on each page. Value range: 0–2000 Default value: 2000
page_reverse	No	Boolean	Specifies whether to use reverse query. Value options: • **true**: Query the previous page. • **false** (default): Query the next page. Note: • This parameter must be used together with **limit**. • If **page_reverse** is set to **true** and you want to query the previous page, set the value of **marker** to the value of **previous_marker**.

Parameter	Mandatory	Type	Description
description	No	Array of strings	Provides supplementary information about the backend server group. Multiple descriptions can be queried in the format of *description=xxx&description=xxx*.
admin_state_up	No	Boolean	Specifies the administrative status of the backend server group.
healthmonitor_id	No	Array of strings	Specifies the ID of the health check configured for the backend server group. Multiple IDs can be queried in the format of *healthmonitor_id=xxx&healthmonitor_id=xxx*.
id	No	Array of strings	Specifies the ID of the backend server group. Multiple IDs can be queried in the format of *id=xxx&id=xxx*.
name	No	Array of strings	Specifies the backend server group name. Multiple names can be queried in the format of *name=xxx&name=xxx*.
loadbalancer_id	No	Array of strings	Specifies the ID of the load balancer with which the backend server group is associated. Multiple IDs can be queried in the format of *loadbalancer_id=xxx&loadbalancer_id=xxx*.
protocol	No	Array of strings	Specifies the protocol used by the backend server group to receive requests from the load balancer. The value can be **TCP**, **UDP**, **TLS**, **HTTP**, **HTTPS**, **GRPC**, or **QUIC**. Multiple protocols can be queried in the format of *protocol=xxx&protocol=xxx*.

Parameter	Mandatory	Type	Description
lb_algorithm	No	Array of strings	Specifies the load balancing algorithm used by the load balancer to route requests to backend servers in the associated backend server group. Value options: • **ROUND_ROBIN**: weighted round robin • **LEAST_CONNECTIONS**: weighted least connections • **SOURCE_IP**: source IP hash • **QUIC_CID**: connection ID Multiple algorithms can be queried in the format of *lb_algorithm=xxx&lb_algorithm=xxx*.
enterprise_project_id	No	Array of strings	Specifies the ID of the enterprise project. • If **enterprise_project_id** is not specified, resources in all enterprise projects are queried by default. Fine-grained authorization is performed. The **elb:pools:list** permission must be assigned to the user group. • If **enterprise_project_id** is specified, the value can be a specific enterprise project ID or **all_granted_eps**. If the value is a specific enterprise project ID, only resources in the enterprise project are queried. If the value is **all_granted_eps**, resources in the enterprise projects with the **elb:pools:list** permission are queried. Multiple values can be queried in the format of *enterprise_project_id=xxx&enterprise_project_id=xxx*.

Parameter	Mandatory	Type	Description
ip_version	No	Array of strings	Specifies the IP address version supported by the backend server group. Multiple versions can be queried in the format of *ip_version=xxx&ip_version=xxx*.
member_address	No	Array of strings	Specifies the private IP address bound to the backend server. This is a query parameter and will not be included in the response. Multiple IP addresses can be queried in the format of *member_address=xxx&member_address=xxx*.
member_device_id	No	Array of strings	Specifies the ID of the cloud server that serves as a backend server. This parameter is used only as a query condition and is not included in the response. Multiple IDs can be queried in the format of *member_device_id=xxx&member_device_id=xxx*.
member_deletion_protection_enable	No	Boolean	Specifies whether to enable deletion protection. Value options: • **true**: Enable deletion protection. • **false** (default): Disable deletion protection.
listener_id	No	Array of strings	Specifies the IDs of the associated listeners, including the listeners associated through forwarding policies. Multiple IDs can be queried in the format of *listener_id=xxx&listener_id=xxx*.

Parameter	Mandatory	Type	Description
member_instance_id	No	Array of strings	Specifies the backend server ID. This parameter is used only as a query condition and is not included in the response. Multiple IDs can be queried in the format of *member_instance_id=xxx&member_instance_id=xxx*.
vpc_id	No	Array of strings	Specifies the ID of the VPC where the backend server group works.
type	No	Array of strings	Specifies the type of the backend server group. Value options: • **instance**: Any type of backend servers can be added. **vpc_id** is mandatory. • **ip**: Only IP as backend servers can be added. **vpc_id** cannot be specified. • **""**: Any type of backend servers can be added.
protection_status	No	Array of strings	Specifies the protection status. Value options: • **nonProtection** (default): The load balancer is not protected. • **consoleProtection**: **Modification Protection** is enabled on the console.
connection_drain	No	Boolean	Specifies a **connection_drain** value for query, in the format of **connection_drain=true** or **connection_drain=false**.
pool_health	No	String	This API is used to query whether **pool_health** is enabled. If **minimum_healthy_member_count** is **0**, **pool_health** is disabled. If **minimum_healthy_member_count** is **1**, **pool_health** is enabled.

Parameter	Mandatory	Type	Description
any_port_enable	No	Boolean	Specifies whether to enable **Forward to Same Port** for a backend server group. If this option is enabled, the listener routes the requests to the backend server over the same port as the frontend port. Value options: • **false**: Disable this option. • **true**: Enable this option.
public_border_group	No	String	Specifies the public border group.
quic_cid_len	No	Integer	Specifies the QUIC connection ID that is used to query backend server groups. It is used only as a query condition but not as a response parameter. Multiple values can be queried in the format of *quic_cid_len=3&quic_cid_len=5*.
quic_cid_offset	No	Integer	Specifies the QUIC connection ID offset that is used to query backend server groups. It is used only as a query condition but not as a response parameter. Multiple values can be queried in the format of *quic_cid_offset=1&quic_cid_offset=3*.

Request Parameters

Table 5-361 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-362 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
page_info	**PageInfo** object	Shows pagination information.
pools	Array of **Pool** objects	Lists the backend server groups.

Table 5-363 PageInfo

Parameter	Type	Description
previous_marker	String	Specifies the ID of the first record in the pagination query result. When **page_reverse** is set to **true**, this parameter is used together to query resources on the previous page.
next_marker	String	Specifies the ID of the last record in the pagination query result.
current_count	Integer	Specifies the number of records.

Table 5-364 Pool

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the backend server group.
description	String	Provides supplementary information about the backend server group.
healthmonitor_id	String	Specifies the ID of the health check configured for the backend server group.
id	String	Specifies the backend server group ID.

Parameter	Type	Description
lb_algorithm	String	Specifies the load balancing algorithm used by the load balancer to route requests to backend servers in the associated backend server group. Value options: • **ROUND_ROBIN**: weighted round robin • **LEAST_CONNECTIONS**: weighted least connections • **SOURCE_IP**: source IP hash • **QUIC_CID**: connection ID
listeners	Array of **ListenerRef** objects	Specifies the IDs of the listeners with which the backend server group is associated.
loadbalancers	Array of **LoadBalancerRef** objects	Specifies the IDs of the load balancers with which the backend server group is associated.
members	Array of **MemberRef** objects	Specifies the IDs of the backend servers in the backend server group.
name	String	Specifies the backend server group name.
project_id	String	Specifies the project ID.

Parameter	Type	Description
protocol	String	Specifies the protocol used by the backend server group to receive requests. The value can be **TCP**, **UDP**, **TLS**, **HTTP**, **HTTPS**, **GRPC**, or **QUIC**. Note: • If the listener's protocol is **UDP**, the protocol of the backend server group must be **UDP** or **QUIC**. • If the listener's protocol is **TCP**, the protocol of the backend server group must be **TCP**. • If the listener's protocol is **HTTP**, the protocol of the backend server group must be **HTTP**. • If the listener's protocol is **HTTPS**, the protocol of the backend server group can be **HTTP**, **HTTPS**, or **GRPC**. • If the listener's protocol is **TERMINATED_HTTPS**, the protocol of the backend server group must be **HTTP**. • If the listener's protocol is **QUIC**, the protocol of the backend server group can be **HTTP**, **HTTPS**, or **GRPC**. • If the listener's protocol is **TLS**, the protocol of the backend server group can be **TLS** or **TCP**. If protocol of the backend server group is TCP, the **ip_version** must be set to **v4**. Note: • If protocol of the backend server group is QUIC, **session_persistence** must be set to **true**, with **type** set to **SOURCE_IP**. • If protocol of the backend server group is GRPC, **http2_enable** of the listener must be set to **true**.
session_persistence	**SessionPersistence** object	Specifies the sticky session.

Parameter	Type	Description
ip_version	String	Specifies the IP address version supported by the backend server group. Value range: • Shared load balancers: The value is fixed at **v4**. • Dedicated load balancers: The value can be **dualstack** or **v4**. If the protocol of the backend server group is TCP or UDP, the value is **dualstack**. If the protocol of the backend server group is HTTP, the value is **v4**.
slow_start	**SlowStart** object	Specifies slow start details. After you enable slow start, new backend servers added to the backend server group are warmed up, and the number of requests they can receive increases linearly during the configured slow start duration. This parameter can be used when the protocol of the backend server group is HTTP or HTTPS. An error will be returned if the protocol is not HTTP or HTTPS.
member_deletion_protection_enable	Boolean	Specifies whether to enable deletion protection. Value options: • **true**: Enable deletion protection. • **false**: Disable deletion protection. **NOTE** Disable deletion protection for all your resources before deleting your account.
created_at	String	Specifies the time when the backend server group was created. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.

Parameter	Type	Description
updated_at	String	Specifies the time when the backend server group was updated. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
vpc_id	String	Specifies the ID of the VPC where the backend server group works.
type	String	Specifies the type of the backend server group. Value options: ● **instance**: Any type of backend servers can be added. **vpc_id** is mandatory. ● **ip**: Only IP as backend servers can be added. **vpc_id** cannot be specified. ● **""**: Any type of backend servers can be added.
protection_status	String	Specifies the protection status. Value options: ● **nonProtection** (default): The load balancer is not protected. ● **consoleProtection**: **Modification Protection** is enabled on the console.
protection_reason	String	Specifies why the modification protection is enabled. Note: This parameter is valid only when **protection_status** is set to **consoleProtection**. The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).

Parameter	Type	Description
any_port_enable	Boolean	Specifies whether to enable **any_port_enable** for a backend server group. If this option is enabled, the listener routes the requests to the backend server over the same port as the frontend port. If this option is disabled, the listener routes the requests over the port specified by **protocol_port**. Value options: • **false**: Disable this option. • **true**: Enable this option. Note: This option is available only for TCP, UDP, or QUIC backend server groups.
connection_drain	**ConnectionDrain** object	Specifies the configurations of deregistration delay. This parameter is only available for TCP, UDP, and QUIC backend server groups and TCP and UDP listeners. This parameter takes effect when: • A backend server is removed from a backend server group. • A backend server is detected unhealthy or health checks fail. • The weight of a backend server is 0.
enterprise_project_id	String	Specifies the ID of the enterprise project that the IP address group belongs to.
pool_health	**PoolHealth** object	Specifies the configurations of the pool health feature.
public_border_group	String	Specifies the public border group, for example, **center**.
quic_cid_hash_strategy	**QuicCidHashStrategy** object	Specifies multi-path forwarding policy based on destination connection IDs.

Table 5-365 ListenerRef

Parameter	Type	Description
id	String	Specifies the listener ID.

Table 5-366 LoadBalancerRef

Parameter	Type	Description
id	String	Specifies the load balancer ID.

Table 5-367 MemberRef

Parameter	Type	Description
id	String	Specifies the backend server ID.

Table 5-368 SessionPersistence

Parameter	Type	Description
cookie_name	String	Specifies the cookie name. Note: • This parameter will take effect only when **type** is set to **APP_COOKIE**. Otherwise, an error will be returned. Value ranges: • For shared load balancers, the name can contain a maximum of 64 characters, including letters, digits, underscores (_), and hyphens (-). • For dedicated load balancers, the name can contain a maximum of 255 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).

Parameter	Type	Description
type	String	Specifies the sticky session type. The value can be **SOURCE_IP**, **HTTP_COOKIE**, or **APP_COOKIE**. Note: • If the protocol of the backend server group is **TCP** or **UDP**, only **SOURCE_IP** takes effect. • If the protocol of the backend server group is **HTTP** or **HTTPS**, the value can be **HTTP_COOKIE** or **APP_COOKIE**. • If the backend server group protocol is **QUIC**, sticky session must be enabled with **type** set to **SOURCE_IP**.
persistence_timeout	Integer	Specifies the stickiness duration, in minutes. This parameter will not take effect when **type** is set to **APP_COOKIE**. • If the protocol of the backend server group is TCP, UDP, or QUIC, the value ranges from **1** to **60**, and the default value is **1**. • If the protocol of the backend server group is HTTP or HTTPS, the value ranges from **1** to **1440**, and the default value is **1440**.

Table 5-369 SlowStart

Parameter	Type	Description
enable	Boolean	Specifies whether to enable slow start. • **true**: Enable slow start. • **false** (default): Disable slow start.
duration	Integer	Specifies the slow start duration, in seconds. The value ranges from **30** to **1200**, and the default value is **30**.

Table 5-370 ConnectionDrain

Parameter	Type	Description
enable	Boolean	Specifies whether to enable **connection_drain**. Value options: • **true**: Enable this option. • **false**: Disable this option. Default value: **true**
timeout	Integer	Specifies the deregistration delay timeout, in seconds. The value ranges from **10** to **4000**.

Table 5-371 PoolHealth

Parameter	Type	Description
minimum_healthy_member_count	Integer	If the number of healthy backend servers is less than the value specified for this parameter, the backend server group is considered as unhealthy. The value can be **0** (disabled) or **1** (enabled).

Table 5-372 QuicCidHashStrategy

Parameter	Type	Description
len	Integer	Specifies the length of the hash factor in the connection ID, in byte. This parameter is valid only when the load balancing algorithm is **QUIC_CID**. Value range: 1 to 20 Default value: 3
offset	Integer	Specifies the start position in the connection ID as the hash factor, in byte. This parameter is valid only when the load balancing algorithm is **QUIC_CID**. Value range: 0 to 19 Default value: 1

Example Requests

Querying backend server groups

```
GET https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/pools?limit=2
```

Example Responses

Status code: 200

Successful request.


```
{
  "pools" : [ {
    "lb_algorithm" : "ROUND_ROBIN",
    "protocol" : "HTTP",
    "type" : "",
    "vpc_id" : "",
    "description" : "",
    "admin_state_up" : true,
    "member_deletion_protection_enable" : false,
    "loadbalancers" : [ {
      "id" : "309a0f61-0b62-45f2-97d1-742f3434338e"
    } ],
    "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
    "session_persistence" : {
      "cookie_name" : "my_cookie",
      "type" : "APP_COOKIE",
      "persistence_timeout" : 1
    },
    "healthmonitor_id" : "",
    "listeners" : [ ],
    "members" : [ ],
    "id" : "73bd4fe0-ffbb-4b56-aab4-4f26ddf7a103",
    "name" : "",
    "ip_version" : "v4",
    "pool_health" : {
      "minimum_healthy_member_count" : 0
    }
  }, {
    "lb_algorithm" : "SOURCE_IP",
    "protocol" : "TCP",
    "description" : "",
    "admin_state_up" : true,
    "member_deletion_protection_enable" : false,
    "loadbalancers" : [ {
      "id" : "d9763e59-64b7-4e93-aec7-0ff7881ef9bc"
    } ],
    "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
    "session_persistence" : {
      "cookie_name" : "",
      "type" : "SOURCE_IP",
      "persistence_timeout" : 1
    },
    "healthmonitor_id" : "",
    "listeners" : [ {
      "id" : "8d21db6f-b475-429e-a9cb-90439b0413b2"
    } ],
    "members" : [ ],
    "id" : "74db02d1-5711-4c77-b383-a450e2b93142",
    "name" : "pool_tcp_001",
    "ip_version" : "dualstack",
    "pool_health" : {
      "minimum_healthy_member_count" : 0
    }
  } ],
  "page_info" : {
    "next_marker" : "74db02d1-5711-4c77-b383-a450e2b93142",
```



```
    "previous_marker" : "73bd4fe0-ffbb-4b56-aab4-4f26ddf7a103",
    "current_count" : 2
  },
  "request_id" : "a1a7e852-1928-48f7-bbc9-ca8469898713"
}
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ListPoolsSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ListPoolsRequest request = new ListPoolsRequest();
        try {
            ListPoolsResponse response = client.listPools(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListPoolsRequest()
        response = client.list_pools(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListPoolsRequest{}
    response, err := client.ListPools(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	Successful request.

Error Codes

See **Error Codes**.

5.11.3 Querying the Details of a Backend Server Group

Function

This API is used to view the details of a backend server group.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/pools/{pool_id}

Table 5-373 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
pool_id	Yes	String	Specifies the ID of the backend server group.

Request Parameters

Table 5-374 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-375 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
pool	**Pool** object	Specifies the backend server group.

Table 5-376 Pool

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the backend server group.
description	String	Provides supplementary information about the backend server group.
healthmonitor_id	String	Specifies the ID of the health check configured for the backend server group.
id	String	Specifies the backend server group ID.

Parameter	Type	Description
lb_algorithm	String	Specifies the load balancing algorithm used by the load balancer to route requests to backend servers in the associated backend server group. Value options: • **ROUND_ROBIN**: weighted round robin • **LEAST_CONNECTIONS**: weighted least connections • **SOURCE_IP**: source IP hash • **QUIC_CID**: connection ID
listeners	Array of **ListenerRef** objects	Specifies the IDs of the listeners with which the backend server group is associated.
loadbalancers	Array of **LoadBalancerRef** objects	Specifies the IDs of the load balancers with which the backend server group is associated.
members	Array of **MemberRef** objects	Specifies the IDs of the backend servers in the backend server group.
name	String	Specifies the backend server group name.
project_id	String	Specifies the project ID.

Parameter	Type	Description
protocol	String	Specifies the protocol used by the backend server group to receive requests. The value can be **TCP**, **UDP**, **TLS**, **HTTP**, **HTTPS**, **GRPC**, or **QUIC**. Note: • If the listener's protocol is **UDP**, the protocol of the backend server group must be **UDP** or **QUIC**. • If the listener's protocol is **TCP**, the protocol of the backend server group must be **TCP**. • If the listener's protocol is **HTTP**, the protocol of the backend server group must be **HTTP**. • If the listener's protocol is **HTTPS**, the protocol of the backend server group can be **HTTP**, **HTTPS**, or **GRPC**. • If the listener's protocol is **TERMINATED_HTTPS**, the protocol of the backend server group must be **HTTP**. • If the listener's protocol is **QUIC**, the protocol of the backend server group can be **HTTP**, **HTTPS**, or **GRPC**. • If the listener's protocol is **TLS**, the protocol of the backend server group can be **TLS** or **TCP**. If protocol of the backend server group is TCP, the **ip_version** must be set to **v4**. Note: • If protocol of the backend server group is QUIC, **session_persistence** must be set to **true**, with **type** set to **SOURCE_IP**. • If protocol of the backend server group is GRPC, **http2_enable** of the listener must be set to **true**.
session_persistence	**SessionPersistence** object	Specifies the sticky session.

Parameter	Type	Description
ip_version	String	Specifies the IP address version supported by the backend server group. Value range: • Shared load balancers: The value is fixed at **v4**. • Dedicated load balancers: The value can be **dualstack** or **v4**. If the protocol of the backend server group is TCP or UDP, the value is **dualstack**. If the protocol of the backend server group is HTTP, the value is **v4**.
slow_start	**SlowStart** object	Specifies slow start details. After you enable slow start, new backend servers added to the backend server group are warmed up, and the number of requests they can receive increases linearly during the configured slow start duration. This parameter can be used when the protocol of the backend server group is HTTP or HTTPS. An error will be returned if the protocol is not HTTP or HTTPS.
member_deletion_protection_enable	Boolean	Specifies whether to enable deletion protection. Value options: • **true**: Enable deletion protection. • **false**: Disable deletion protection. **NOTE** Disable deletion protection for all your resources before deleting your account.
created_at	String	Specifies the time when the backend server group was created. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.

Parameter	Type	Description
updated_at	String	Specifies the time when the backend server group was updated. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
vpc_id	String	Specifies the ID of the VPC where the backend server group works.
type	String	Specifies the type of the backend server group. Value options: ● **instance**: Any type of backend servers can be added. **vpc_id** is mandatory. ● **ip**: Only IP as backend servers can be added. **vpc_id** cannot be specified. ● **""**: Any type of backend servers can be added.
protection_status	String	Specifies the protection status. Value options: ● **nonProtection** (default): The load balancer is not protected. ● **consoleProtection**: **Modification Protection** is enabled on the console.
protection_reason	String	Specifies why the modification protection is enabled. Note: This parameter is valid only when **protection_status** is set to **consoleProtection**. The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).

Parameter	Type	Description
any_port_enable	Boolean	Specifies whether to enable **any_port_enable** for a backend server group. If this option is enabled, the listener routes the requests to the backend server over the same port as the frontend port. If this option is disabled, the listener routes the requests over the port specified by **protocol_port**. Value options: • **false**: Disable this option. • **true**: Enable this option. Note: This option is available only for TCP, UDP, or QUIC backend server groups.
connection_drain	**ConnectionDrain** object	Specifies the configurations of deregistration delay. This parameter is only available for TCP, UDP, and QUIC backend server groups and TCP and UDP listeners. This parameter takes effect when: • A backend server is removed from a backend server group. • A backend server is detected unhealthy or health checks fail. • The weight of a backend server is 0.
enterprise_project_id	String	Specifies the ID of the enterprise project that the IP address group belongs to.
pool_health	**PoolHealth** object	Specifies the configurations of the pool health feature.
public_border_group	String	Specifies the public border group, for example, **center**.
quic_cid_hash_strategy	**QuicCidHashStrategy** object	Specifies multi-path forwarding policy based on destination connection IDs.

Table 5-377 ListenerRef

Parameter	Type	Description
id	String	Specifies the listener ID.

Table 5-378 LoadBalancerRef

Parameter	Type	Description
id	String	Specifies the load balancer ID.

Table 5-379 MemberRef

Parameter	Type	Description
id	String	Specifies the backend server ID.

Table 5-380 SessionPersistence

Parameter	Type	Description
cookie_name	String	Specifies the cookie name. Note: • This parameter will take effect only when **type** is set to **APP_COOKIE**. Otherwise, an error will be returned. Value ranges: • For shared load balancers, the name can contain a maximum of 64 characters, including letters, digits, underscores (_), and hyphens (-). • For dedicated load balancers, the name can contain a maximum of 255 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).

Parameter	Type	Description
type	String	Specifies the sticky session type. The value can be **SOURCE_IP**, **HTTP_COOKIE**, or **APP_COOKIE**. Note: • If the protocol of the backend server group is **TCP** or **UDP**, only **SOURCE_IP** takes effect. • If the protocol of the backend server group is **HTTP** or **HTTPS**, the value can be **HTTP_COOKIE** or **APP_COOKIE**. • If the backend server group protocol is **QUIC**, sticky session must be enabled with **type** set to **SOURCE_IP**.
persistence_timeout	Integer	Specifies the stickiness duration, in minutes. This parameter will not take effect when **type** is set to **APP_COOKIE**. • If the protocol of the backend server group is TCP, UDP, or QUIC, the value ranges from **1** to **60**, and the default value is **1**. • If the protocol of the backend server group is HTTP or HTTPS, the value ranges from **1** to **1440**, and the default value is **1440**.

Table 5-381 SlowStart

Parameter	Type	Description
enable	Boolean	Specifies whether to enable slow start. • **true**: Enable slow start. • **false** (default): Disable slow start.
duration	Integer	Specifies the slow start duration, in seconds. The value ranges from **30** to **1200**, and the default value is **30**.

Table 5-382 ConnectionDrain

Parameter	Type	Description
enable	Boolean	Specifies whether to enable **connection_drain**. Value options: • **true**: Enable this option. • **false**: Disable this option. Default value: **true**
timeout	Integer	Specifies the deregistration delay timeout, in seconds. The value ranges from **10** to **4000**.

Table 5-383 PoolHealth

Parameter	Type	Description
minimum_healthy_member_count	Integer	If the number of healthy backend servers is less than the value specified for this parameter, the backend server group is considered as unhealthy. The value can be **0** (disabled) or **1** (enabled).

Table 5-384 QuicCidHashStrategy

Parameter	Type	Description
len	Integer	Specifies the length of the hash factor in the connection ID, in byte. This parameter is valid only when the load balancing algorithm is **QUIC_CID**. Value range: 1 to 20 Default value: 3
offset	Integer	Specifies the start position in the connection ID as the hash factor, in byte. This parameter is valid only when the load balancing algorithm is **QUIC_CID**. Value range: 0 to 19 Default value: 1

Example Requests

Querying the details of a backend server group

```
GET https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/pools/36ce7086-a496-4666-9064-5ba0e6840c75
```

Example Responses

Status code: 200

Successful request.


```
{
  "pool" : {
    "type" : "",
    "vpc_id" : "",
    "lb_algorithm" : "LEAST_CONNECTIONS",
    "protocol" : "TCP",
    "description" : "My pool",
    "admin_state_up" : true,
    "member_deletion_protection_enable" : false,
    "loadbalancers" : [ {
      "id" : "098b2f68-af1c-41a9-8efd-69958722af62"
    } ],
    "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
    "session_persistence" : null,
    "healthmonitor_id" : "",
    "listeners" : [ {
      "id" : "0b11747a-b139-492f-9692-2df0b1c87193"
    }, {
      "id" : "61942790-2367-482a-8b0e-93840ea2a1c6"
    }, {
      "id" : "fd8f954c-f0f8-4d39-bb1d-41637cd6b1be"
    } ],
    "members" : [ ],
    "id" : "36ce7086-a496-4666-9064-5ba0e6840c75",
    "name" : "My pool.",
    "ip_version" : "dualstack",
    "pool_health" : {
      "minimum_healthy_member_count" : 0
    }
  },
  "request_id" : "c1a60da2-1ec7-4a1c-b4cc-73e1a57b368e"
}
```


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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ShowPoolSolution {
```



```
    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowPoolRequest request = new ShowPoolRequest();
        request.withPoolId("{pool_id}");
        try {
            ShowPoolResponse response = client.showPool(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowPoolRequest()
        request.pool_id = "{pool_id}"
        response = client.show_pool(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowPoolRequest{}
    request.PoolId = "{pool_id}"
    response, err := client.ShowPool(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	Successful request.

Error Codes

See **Error Codes**.

5.11.4 Updating a Backend Server Group

Function

This API is used to update a backend server group.

Constraints

The backend server group can be updated only when the provisioning status of the associated load balancer is **ACTIVE**.

Calling Method

For details, see **Calling APIs**.

URI

PUT /v3/{project_id}/elb/pools/{pool_id}

Table 5-385 Path Parameters

Parameter	Mandatory	Type	Description
pool_id	Yes	String	Specifies the backend server group ID.
project_id	Yes	String	Specifies the project ID.

Request Parameters

Table 5-386 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Table 5-387 Request body parameters

Parameter	Mandatory	Type	Description
pool	Yes	**UpdatePoolOption** object	Specifies the backend server group.

Table 5-388 UpdatePoolOption

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Specifies the administrative status of the backend server group. The value can only be updated to **true**.
description	No	String	Provides supplementary information about the backend server group.
lb_algorithm	No	String	Specifies the load balancing algorithm used by the load balancer to route requests to backend servers in the associated backend server group. Value options: • **ROUND_ROBIN**: weighted round robin • **LEAST_CONNECTIONS**: weighted least connections • **SOURCE_IP**: source IP hash • **QUIC_CID**: connection ID
name	No	String	Specifies the backend server group name.
session_persistence	No	**UpdatePoolSessionPersistenceOption** object	Specifies the sticky session.
slow_start	No	**UpdatePoolSlowStartOption** object	Specifies slow start details. After you enable slow start, new backend servers added to the backend server group are warmed up, and the number of requests they can receive increases linearly during the configured slow start duration. Note: This parameter can be used when the protocol of the backend server group is HTTP or HTTPS.

Parameter	Mandatory	Type	Description
member_deletion_protection_enable	No	Boolean	Specifies whether to enable deletion protection. Value options: • **true**: Enable deletion protection. • **false**: Disable deletion protection. **NOTE** Disable deletion protection for all your resources before deleting your account.
vpc_id	No	String	Specifies the ID of the VPC where the backend server group works. This parameter can be updated only when **vpc_id** is left blank.
type	No	String	Specifies the type of the backend server group. Value options: • **instance**: Any type of backend servers can be added. **vpc_id** is mandatory. • **ip**: Only IP as backend servers can be added. **vpc_id** cannot be specified. • **""**: Any type of backend servers can be added. Note: This parameter can be updated only when **type** is left blank.
protection_status	No	String	Specifies the protection status. Value options: • **nonProtection**: The load balancer is not protected. • **consoleProtection**: **Modification Protection** is enabled on the console.

Parameter	Mandatory	Type	Description
protection_reason	No	String	Specifies why the modification protection is enabled. Note: This parameter is valid only when **protection_status** is set to **consoleProtection**. The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).
any_port_enable	No	Boolean	Specifies whether to enable **any_port_enable** for a backend server group. If this option is enabled, the listener routes the requests to the backend server over the same port as the frontend port. If this option is disabled, the listener routes the requests over the port specified by **protocol_port**. Value options: • **false**: Disable this option. • **true**: Enable this option. Note: This option is available only for TCP, UDP, or QUIC backend server groups.
connection_drain	No	**ConnectionDrain** object	Specifies the configurations of deregistration delay. This parameter is only available for TCP, UDP, and QUIC backend server groups and TCP and UDP listeners. This parameter takes effect when: • A backend server is removed from a backend server group. • A backend server is detected unhealthy or health checks fail. • The weight of a backend server is 0.
pool_health	No	**PoolHealth** object	Specifies the configurations of the pool health feature.

Parameter	Mandatory	Type	Description
quic_cid_hash_strategy	No	QuicCidHashStrategy object	Specifies multi-path distribution configuration based on destination connection IDs.

Table 5-389 UpdatePoolSessionPersistenceOption

Parameter	Mandatory	Type	Description
cookie_name	No	String	Specifies the cookie name. Note: • This parameter will take effect only when **type** is set to **APP_COOKIE**. Otherwise, an error will be returned. Value ranges: • For shared load balancers, the name can contain a maximum of 64 characters, including letters, digits, underscores (_), and hyphens (-). • For dedicated load balancers, the name can contain a maximum of 255 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).

Parameter	Mandatory	Type	Description
type	No	String	Specifies the sticky session type. The value can be **SOURCE_IP**, **HTTP_COOKIE**, or **APP_COOKIE**.Note: • If the protocol of the backend server group is **TCP** or **UDP**, only **SOURCE_IP** takes effect. • For dedicated load balancers, if the protocol of the backend server group is **HTTP** or **HTTPS**, the value can only be **HTTP_COOKIE**. • If the backend server group protocol is **QUIC**, sticky session must be enabled with **type** set to **SOURCE_IP**.
persistence_timeout	No	Integer	Specifies the stickiness duration, in minutes. This parameter will not take effect when **type** is set to **APP_COOKIE**. • If the protocol of the backend server group is TCP, UDP, or QUIC, the value ranges from **1** to **60**, and the default value is **1**. • If the protocol of the backend server group is HTTP or HTTPS, the value ranges from **1** to **1440**, and the default value is **1440**.

Table 5-390 UpdatePoolSlowStartOption

Parameter	Mandatory	Type	Description
enable	No	Boolean	Specifies whether to enable slow start. • **true**: Enable slow start. • **false** (default): Disable slow start.

Parameter	Mandatory	Type	Description
duration	No	Integer	Specifies the slow start duration, in seconds. The value ranges from **30** to **1200**, and the default value is **30**.

Table 5-391 ConnectionDrain

Parameter	Mandatory	Type	Description
enable	No	Boolean	Specifies whether to enable **connection_drain**. Value options: • **true**: Enable this option. • **false**: Disable this option. Default value: **true**
timeout	No	Integer	Specifies the deregistration delay timeout, in seconds. The value ranges from **10** to **4000**.

Table 5-392 PoolHealth

Parameter	Mandatory	Type	Description
minimum_healthy_member_count	No	Integer	If the number of healthy backend servers is less than the value specified for this parameter, the backend server group is considered as unhealthy. The value can be **0** (disabled) or **1** (enabled).

Table 5-393 QuicCidHashStrategy

Parameter	Mandatory	Type	Description
len	Yes	Integer	Specifies the length of the hash factor in the connection ID, in byte. This parameter is valid only when the load balancing algorithm is **QUIC_CID**. Value range: 1 to 20 Default value: 3
offset	Yes	Integer	Specifies the start position in the connection ID as the hash factor, in byte. This parameter is valid only when the load balancing algorithm is **QUIC_CID**. Value range: 0 to 19 Default value: 1

Response Parameters

Status code: 200

Table 5-394 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
pool	**Pool** object	Specifies the backend server group.

Table 5-395 Pool

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the backend server group.
description	String	Provides supplementary information about the backend server group.
healthmonitor_id	String	Specifies the ID of the health check configured for the backend server group.

Parameter	Type	Description
id	String	Specifies the backend server group ID.
lb_algorithm	String	Specifies the load balancing algorithm used by the load balancer to route requests to backend servers in the associated backend server group. Value options: • **ROUND_ROBIN**: weighted round robin • **LEAST_CONNECTIONS**: weighted least connections • **SOURCE_IP**: source IP hash • **QUIC_CID**: connection ID
listeners	Array of **ListenerRef** objects	Specifies the IDs of the listeners with which the backend server group is associated.
loadbalancers	Array of **LoadBalancerRef** objects	Specifies the IDs of the load balancers with which the backend server group is associated.
members	Array of **MemberRef** objects	Specifies the IDs of the backend servers in the backend server group.
name	String	Specifies the backend server group name.
project_id	String	Specifies the project ID.

Parameter	Type	Description
protocol	String	Specifies the protocol used by the backend server group to receive requests. The value can be **TCP**, **UDP**, **TLS**, **HTTP**, **HTTPS**, **GRPC**, or **QUIC**. Note: • If the listener's protocol is **UDP**, the protocol of the backend server group must be **UDP** or **QUIC**. • If the listener's protocol is **TCP**, the protocol of the backend server group must be **TCP**. • If the listener's protocol is **HTTP**, the protocol of the backend server group must be **HTTP**. • If the listener's protocol is **HTTPS**, the protocol of the backend server group can be **HTTP**, **HTTPS**, or **GRPC**. • If the listener's protocol is **TERMINATED_HTTPS**, the protocol of the backend server group must be **HTTP**. • If the listener's protocol is **QUIC**, the protocol of the backend server group can be **HTTP**, **HTTPS**, or **GRPC**. • If the listener's protocol is **TLS**, the protocol of the backend server group can be **TLS** or **TCP**. If protocol of the backend server group is TCP, the **ip_version** must be set to **v4**. Note: • If protocol of the backend server group is QUIC, **session_persistence** must be set to **true**, with **type** set to **SOURCE_IP**. • If protocol of the backend server group is GRPC, **http2_enable** of the listener must be set to **true**.
session_persistence	**SessionPersistence** object	Specifies the sticky session.

Parameter	Type	Description
ip_version	String	Specifies the IP address version supported by the backend server group. Value range: • Shared load balancers: The value is fixed at **v4**. • Dedicated load balancers: The value can be **dualstack** or **v4**. If the protocol of the backend server group is TCP or UDP, the value is **dualstack**. If the protocol of the backend server group is HTTP, the value is **v4**.
slow_start	**SlowStart** object	Specifies slow start details. After you enable slow start, new backend servers added to the backend server group are warmed up, and the number of requests they can receive increases linearly during the configured slow start duration. This parameter can be used when the protocol of the backend server group is HTTP or HTTPS. An error will be returned if the protocol is not HTTP or HTTPS.
member_deletion_protection_enable	Boolean	Specifies whether to enable deletion protection. Value options: • **true**: Enable deletion protection. • **false**: Disable deletion protection. **NOTE** Disable deletion protection for all your resources before deleting your account.
created_at	String	Specifies the time when the backend server group was created. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.

Parameter	Type	Description
updated_at	String	Specifies the time when the backend server group was updated. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
vpc_id	String	Specifies the ID of the VPC where the backend server group works.
type	String	Specifies the type of the backend server group. Value options: ● **instance**: Any type of backend servers can be added. **vpc_id** is mandatory. ● **ip**: Only IP as backend servers can be added. **vpc_id** cannot be specified. ● **""**: Any type of backend servers can be added.
protection_status	String	Specifies the protection status. Value options: ● **nonProtection** (default): The load balancer is not protected. ● **consoleProtection**: **Modification Protection** is enabled on the console.
protection_reason	String	Specifies why the modification protection is enabled. Note: This parameter is valid only when **protection_status** is set to **consoleProtection**. The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).

Parameter	Type	Description
any_port_enable	Boolean	Specifies whether to enable **any_port_enable** for a backend server group. If this option is enabled, the listener routes the requests to the backend server over the same port as the frontend port. If this option is disabled, the listener routes the requests over the port specified by **protocol_port**. Value options: • **false**: Disable this option. • **true**: Enable this option. Note: This option is available only for TCP, UDP, or QUIC backend server groups.
connection_drain	**ConnectionDrain** object	Specifies the configurations of deregistration delay. This parameter is only available for TCP, UDP, and QUIC backend server groups and TCP and UDP listeners. This parameter takes effect when: • A backend server is removed from a backend server group. • A backend server is detected unhealthy or health checks fail. • The weight of a backend server is 0.
enterprise_project_id	String	Specifies the ID of the enterprise project that the IP address group belongs to.
pool_health	**PoolHealth** object	Specifies the configurations of the pool health feature.
public_border_group	String	Specifies the public border group, for example, **center**.
quic_cid_hash_strategy	**QuicCidHashStrategy** object	Specifies multi-path forwarding policy based on destination connection IDs.

Table 5-396 ListenerRef

Parameter	Type	Description
id	String	Specifies the listener ID.

Table 5-397 LoadBalancerRef

Parameter	Type	Description
id	String	Specifies the load balancer ID.

Table 5-398 MemberRef

Parameter	Type	Description
id	String	Specifies the backend server ID.

Table 5-399 SessionPersistence

Parameter	Type	Description
cookie_name	String	Specifies the cookie name. Note: • This parameter will take effect only when **type** is set to **APP_COOKIE**. Otherwise, an error will be returned. Value ranges: • For shared load balancers, the name can contain a maximum of 64 characters, including letters, digits, underscores (_), and hyphens (-). • For dedicated load balancers, the name can contain a maximum of 255 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).

Parameter	Type	Description
type	String	Specifies the sticky session type. The value can be **SOURCE_IP**, **HTTP_COOKIE**, or **APP_COOKIE**. Note: • If the protocol of the backend server group is **TCP** or **UDP**, only **SOURCE_IP** takes effect. • If the protocol of the backend server group is **HTTP** or **HTTPS**, the value can be **HTTP_COOKIE** or **APP_COOKIE**. • If the backend server group protocol is **QUIC**, sticky session must be enabled with **type** set to **SOURCE_IP**.
persistence_timeout	Integer	Specifies the stickiness duration, in minutes. This parameter will not take effect when **type** is set to **APP_COOKIE**. • If the protocol of the backend server group is TCP, UDP, or QUIC, the value ranges from **1** to **60**, and the default value is **1**. • If the protocol of the backend server group is HTTP or HTTPS, the value ranges from **1** to **1440**, and the default value is **1440**.

Table 5-400 SlowStart

Parameter	Type	Description
enable	Boolean	Specifies whether to enable slow start. • **true**: Enable slow start. • **false** (default): Disable slow start.
duration	Integer	Specifies the slow start duration, in seconds. The value ranges from **30** to **1200**, and the default value is **30**.

Table 5-401 ConnectionDrain

Parameter	Type	Description
enable	Boolean	Specifies whether to enable **connection_drain**. Value options: • **true**: Enable this option. • **false**: Disable this option. Default value: **true**
timeout	Integer	Specifies the deregistration delay timeout, in seconds. The value ranges from **10** to **4000**.

Table 5-402 PoolHealth

Parameter	Type	Description
minimum_healthy_member_count	Integer	If the number of healthy backend servers is less than the value specified for this parameter, the backend server group is considered as unhealthy. The value can be **0** (disabled) or **1** (enabled).

Table 5-403 QuicCidHashStrategy

Parameter	Type	Description
len	Integer	Specifies the length of the hash factor in the connection ID, in byte. This parameter is valid only when the load balancing algorithm is **QUIC_CID**. Value range: 1 to 20 Default value: 3
offset	Integer	Specifies the start position in the connection ID as the hash factor, in byte. This parameter is valid only when the load balancing algorithm is **QUIC_CID**. Value range: 0 to 19 Default value: 1

Example Requests

Changing the load balancing algorithm of a backend server group

```
PUT https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/pools/36ce7086-a496-4666-9064-5ba0e6840c75

{
  "pool" : {
    "name" : "My pool.",
    "description" : "My pool update",
    "lb_algorithm" : "LEAST_CONNECTIONS"
  }
}
```

Example Responses

Status code: 200

Successful request.

```
{
  "pool" : {
    "type" : "",
    "vpc_id" : "",
    "lb_algorithm" : "LEAST_CONNECTIONS",
    "protocol" : "TCP",
    "description" : "My pool update",
    "admin_state_up" : true,
    "member_deletion_protection_enable" : false,
    "loadbalancers" : [ {
      "id" : "098b2f68-af1c-41a9-8efd-69958722af62"
    } ],
    "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
    "session_persistence" : null,
    "healthmonitor_id" : null,
    "listeners" : [ {
      "id" : "0b11747a-b139-492f-9692-2df0b1c87193"
    }, {
      "id" : "61942790-2367-482a-8b0e-93840ea2a1c6"
    }, {
      "id" : "fd8f954c-f0f8-4d39-bb1d-41637cd6b1be"
    } ],
    "members" : [ ],
    "id" : "36ce7086-a496-4666-9064-5ba0e6840c75",
    "name" : "My pool.",
    "ip_version" : "dualstack",
    "pool_health" : {
      "minimum_healthy_member_count" : 0
    }
  },
  "request_id" : "8f40128b-c72b-4b64-986a-f7e2c633d75f"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Changing the load balancing algorithm of a backend server group

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class UpdatePoolSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdatePoolRequest request = new UpdatePoolRequest();
        request.withPoolId("{pool_id}");
        UpdatePoolRequestBody body = new UpdatePoolRequestBody();
        UpdatePoolOption poolbody = new UpdatePoolOption();
        poolbody.withDescription("My pool update")
            .withLbAlgorithm("LEAST_CONNECTIONS")
            .withName("My pool.");
        body.withPool(poolbody);
        request.withBody(body);
        try {
            UpdatePoolResponse response = client.updatePool(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

Changing the load balancing algorithm of a backend server group

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdatePoolRequest()
        request.pool_id = "{pool_id}"
        poolbody = UpdatePoolOption(
            description="My pool update",
            lb_algorithm="LEAST_CONNECTIONS",
            name="My pool."
        )
        request.body = UpdatePoolRequestBody(
            pool=poolbody
        )
        response = client.update_pool(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

Changing the load balancing algorithm of a backend server group

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())
```



```
    request := &model.UpdatePoolRequest{}
    request.PoolId = "{pool_id}"
    descriptionPool:= "My pool update"
    lbAlgorithmPool:= "LEAST_CONNECTIONS"
    namePool:= "My pool."
    poolbody := &model.UpdatePoolOption{
        Description: &descriptionPool,
        LbAlgorithm: &lbAlgorithmPool,
        Name: &namePool,
    }
    request.Body = &model.UpdatePoolRequestBody{
        Pool: poolbody,
    }
    response, err := client.UpdatePool(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	Successful request.

Error Codes

See **Error Codes**.

5.11.5 Deleting a Backend Server Group

Function

This API is used to delete a backend server group.

Constraints

A backend server group can be deleted only after all servers are removed from the group, the health check configured for the group is deleted, and the group has no forwarding policies associated.

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v3/{project_id}/elb/pools/{pool_id}

Table 5-404 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
pool_id	Yes	String	Specifies the ID of the backend server group.

Request Parameters

Table 5-405 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

None

Example Requests

Deleting a backend server group

```
DELETE https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/pools/36ce7086-a496-4666-9064-5ba0e6840c75
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;
```



```
public class DeletePoolSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        DeletePoolRequest request = new DeletePoolRequest();
        request.withPoolId("{pool_id}");
        try {
            DeletePoolResponse response = client.deletePool(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()
```



```
    try:
        request = DeletePoolRequest()
        request.pool_id = "{pool_id}"
        response = client.delete_pool(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeletePoolRequest{}
    request.PoolId = "{pool_id}"
    response, err := client.DeletePool(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	Successful request.

Error Codes

See **Error Codes**.

5.11.6 Deleting a Backend Server Group and Associated Resources

Function

This API is used to delete a backend server group and associated resources, including backend servers and health checks.

Constraints

Deleting a backend server group will also delete its associated resources, including backend servers and health checks. The backend server group cannot be associated with a forwarding policy, either.

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v3/{project_id}/elb/pools/{pool_id}/delete-cascade

Table 5-406 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
pool_id	Yes	String	Specifies the ID of the backend server group.

Request Parameters

Table 5-407 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

None

Example Requests

```
DELETE https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/pools/36ce7086-a496-4666-9064-5ba0e6840c75/delete-cascade
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class DeletePoolCascadeSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
```



```
                .build();
        DeletePoolCascadeRequest request = new DeletePoolCascadeRequest();
        request.withPoolId("{pool_id}");
        try {
            DeletePoolCascadeResponse response = client.deletePoolCascade(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeletePoolCascadeRequest()
        request.pool_id = "{pool_id}"
        response = client.delete_pool_cascade(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeletePoolCascadeRequest{}
    request.PoolId = "{pool_id}"
    response, err := client.DeletePoolCascade(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 DELETE operations.

Error Codes

See **Error Codes**.

5.12 Backend Server

5.12.1 Adding a Backend Server

Function

This API is used to add a backend server.

Constraints

When you add backend servers, note the following:

- Two backend servers in the same backend server group must have different IP addresses and ports.
- If no subnets are specified during cloud server creation, IP as backend servers can be added. In this case, **address** must be set to an IPv4 address, the protocol of the backend server group must be TCP, HTTP, or HTTPS, and **IP as a Backend** must have been enabled for the load balancer.
- If a subnet is specified during cloud server creation, the subnet must be in the same VPC where the load balancer resides.
- If the backend server group supports IPv4/IPv6 dual stack, **address** can be an IPv4 address or an IPv6 address. If the backend server group supports only IPv4, **address** can only be an IPv4 address.
- If **type** of the backend server is set to **instance**, **address** must be a private IP address that is not used by any load balancer.

Calling Method

For details, see **Calling APIs**.

URI

POST /v3/{project_id}/elb/pools/{pool_id}/members

Table 5-408 Path Parameters

Parameter	Mandatory	Type	Description
pool_id	Yes	String	Specifies the ID of the backend server group.
project_id	Yes	String	Specifies the project ID.

Request Parameters

Table 5-409 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Table 5-410 Request body parameters

Parameter	Mandatory	Type	Description
member	Yes	CreateMemberOption object	Specifies the backend server.

Table 5-411 CreateMemberOption

Parameter	Mandatory	Type	Description
address	Yes	String	Specifies the private IP address bound to the backend server. Note: • If **subnet_cidr_id** is left blank, **IP as a Backend** is enabled. In this case, the IP address must be an IPv4 address. • If **subnet_cidr_id** is not left blank, the IP address version can be IPv4 or IPv6. It must be in the subnet specified by **subnet_cidr_id**.
admin_state_up	No	Boolean	Specifies the administrative status of the backend server. The value can be **true** or **false**. Although this parameter can be used in the APIs for creating and updating backend servers, its actual value depends on whether ECSs exist. If ECSs exist, the value is **true**. Otherwise, the value is **false**.
name	No	String	Specifies the backend server name. Note: The name is not an ECS name. If this parameter is not specified, an empty value will be returned.
project_id	No	String	Specifies the project ID.

Parameter	Mandatory	Type	Description
protocol_port	No	Integer	Specifies the port used by the backend server to receive requests. Note: • This parameter can be left blank because it does not take effect if **any_port_enable** is set to **true** for a backend server group.
subnet_cidr_id	No	String	Specifies the ID of the IPv4 or IPv6 subnet where the backend server resides. **neutron_subnet_id** defines IPv4 subnets, and **neutron_network_id** defines IPv6 subnets. You can query parameters **neutron_subnet_id** and **neutron_network_id** in the response by calling the API GET https://{VPC_Endpoint}/v1/{project_id}/subnets to get the IPv4 subnet ID and IPv6 subnet ID respectively. Note: • The IPv4 or IPv6 subnet must be in the same VPC as the subnet of the load balancer. • If **ip_target_enable** is set to **true**, this parameter can be left blank. In this case, IP as backend servers must use private IPv4 addresses, and the protocol of the backend server group must be TCP, UDP, TLS, HTTP, HTTPS, QUIC, or GRPC. • If **ip_target_enable** is set to **false**, this parameter must be specified.

Parameter	Mandatory	Type	Description
weight	No	Integer	Specifies the weight of the backend server. Requests are routed to backend servers in the same backend server group based on their weights. The value ranges from **0** to **100**, and the default value is **1**. The larger the weight is, the higher proportion of requests the backend server receives. If the weight is set to 0, the backend server will not accept new requests. If **lb_algorithm** is set to **SOURCE_IP** or **QUIC_CID**, this parameter will not take effect.

Response Parameters

Status code: 201

Table 5-412 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
member	**Member** object	Specifies the backend server.

Table 5-413 Member

Parameter	Type	Description
id	String	Specifies the backend server ID. Note: The value of this parameter is not the ID of the server but an ID automatically generated for the backend server that has already been associated with the load balancer.
name	String	Specifies the backend server name. Note: The name is not an ECS name.

Parameter	Type	Description
project_id	String	Specifies the project ID of the backend server.
admin_state_up	Boolean	Specifies the administrative status of the backend server. The value can be **true** or **false**. Although this parameter can be used in the APIs for creating and updating backend servers, its actual value depends on whether ECSs exist. If ECSs exist, the value is **true**. Otherwise, the value is **false**.
subnet_cidr_id	String	Specifies the ID of the IPv4 or IPv6 subnet where the backend server resides. **neutron_subnet_id** defines IPv4 subnets, and **neutron_network_id** defines IPv6 subnets. You can query parameters **neutron_subnet_id** and **neutron_network_id** in the response by calling the API GET https://{VPC_Endpoint}/v1/{project_id}/subnets to get the IPv4 subnet ID and IPv6 subnet ID respectively. Note: • The IPv4 or IPv6 subnet must be in the same VPC as the subnet of the load balancer. • If **ip_target_enable** is set to **true**, this parameter can be left blank. In this case, IP as backend servers must use private IPv4 addresses, and the protocol of the backend server group must be TCP, UDP, TLS, HTTP, HTTPS, QUIC, or GRPC. • If **ip_target_enable** is set to **false**, this parameter must be specified.
protocol_port	Integer	Specifies the port used by the backend server to receive requests. Note: • This parameter can be left blank because it does not take effect if **any_port_enable** is set to **true** for a backend server group.

Parameter	Type	Description
weight	Integer	Specifies the weight of the backend server. Requests are routed to backend servers in the same backend server group based on their weights. The value ranges from **0** to **100**, and the default value is **1**. The larger the weight is, the higher proportion of requests the backend server receives. If the weight is set to 0, the backend server will not accept new requests. If **lb_algorithm** is set to **SOURCE_IP** or **QUIC_CID**, this parameter will not take effect.
address	String	Specifies the private IP address bound to the backend server. Note: • If **subnet_cidr_id** is left blank, **IP as a Backend** is enabled. In this case, the IP address must be an IPv4 address. • If **subnet_cidr_id** is not left blank, the IP address can be IPv4 or IPv6. It must be in the subnet specified by **subnet_cidr_id**.
ip_version	String	Specifies the IP version supported by the backend server. The value can be **v4** (IPv4) or **v6** (IPv6), depending on the value of **address** returned by the system.
operating_status	String	Specifies the health status of the backend server if **listener_id** under **status** is not specified. Value options: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group to which the backend server belongs. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist.

Parameter	Type	Description
status	Array of **MemberStatus** objects	Specifies the health status of the backend server if **listener_id** under **status** is specified. If **listener_id** under **status** is not specified, **operating_status** of **member** takes precedence.
reason	**MemberHealthCheckFailedReason** object	Specifies why health check fails.
created_at	String	Specifies the time when the backend server was added. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
updated_at	String	Specifies the time when the backend server was updated. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
member_type	String	Specifies the type of the backend server. Value options: • **ip**: IP as backend servers • **instance**: ECSs used as backend servers
instance_id	String	Specifies the ID of the instance associated with the backend server. If this parameter is left blank, the backend server is not a real device. It may be an IP address.

Table 5-414 MemberStatus

Parameter	Type	Description
listener_id	String	Specifies the listener ID.
operating_status	String	Specifies the health status of the backend server. Value options: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group to which the backend server belongs. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist.
reason	**MemberHealthCheckFailedReason** object	Specifies why health check fails.

Table 5-415 MemberHealthCheckFailedReason

Parameter	Type	Description
reason_code	String	Specifies the code of the health check failures. Value options: • **CONNECT_TIMEOUT**: The connection with the backend server times out during a health check. • **CONNECT_REFUSED**: The load balancer rejects connections with the backend server during a health check. • **CONNECT_FAILED**: The load balancer fails to establish connections with the backend server during a health check. • **CONNECT_INTERRUPT**: The load balancer is disconnected from the backend server during a health check. • **SSL_HANDSHAKE_ERROR**: The SSL handshakes with the backend server fail during a health check. • **RECV_RESPONSE_FAILED**: The load balancer fails to receive responses from the backend server during a health check. • **RECV_RESPONSE_TIMEOUT**: The load balancer does not receive responses from the backend server within the timeout duration during a health check. • **SEND_REQUEST_FAILED**: The load balancer fails to send a health check request to the backend server during a health check. • **SEND_REQUEST_TIMEOUT**: The load balancer fails to send a health check request to the backend server within the timeout duration. • **RESPONSE_FORMAT_ERROR**: The load balancer receives invalid responses from the backend server during a health check. • **RESPONSE_MISMATCH**: The response code received from the

Parameter	Type	Description
		backend server is different from the preset code.
expected_response	String	Specifies the expected HTTP status code. This parameter will take effect only when **type** is set to **HTTP**, **HTTPS**, or **GRPC**. The status code cannot be **null** if **reason_code** is **RESPONSE_MISMATCH**. Value ranges: ● A specific status code. If **type** is set to **GRPC**, the status code ranges from 0 to 99. If **type** is set to other values, the status code ranges from 200 to 599. For example, the status code can be **0** or **200**. ● A list of status codes that are separated with commas (,), for example, **200,202** or **0,1**. A maximum of five status codes are supported. ● A status code range. Different ranges are separated with commas (,), for example, **200-204,300-399** or **0-5,10-12,20-30**. A maximum of five ranges are supported.
healthcheck_response	String	Specifies the returned HTTP status code in the response. This parameter will take effect only when **type** is set to **HTTP**, **HTTPS**, or **GRPC**. The status code cannot be **null** if **reason_code** is **RESPONSE_MISMATCH**. Value range: A specific status code. If **type** is set to **GRPC**, the status code ranges from 0 to 99. If **type** is set to other values, the status code ranges from 200 to 599. For example, the status code can be **0** or **200**.

Example Requests

- Example 1: Adding a backend server


```
POST https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/pools/36ce7086-a496-4666-9064-5ba0e6840c75/members

{
  "member" : {
    "subnet_cidr_id" : "c09f620e-3492-4429-ac15-445d5dd9ca74",
    "protocol_port" : 89,
    "name" : "My member",
    "address" : "120.10.10.16"
  }
}
```

- Example 2: Adding an IP address as a backend server

```
POST https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/pools/36ce7086-a496-4666-9064-5ba0e6840c75/members

{
  "member" : {
    "protocol_port" : 89,
    "name" : "My member",
    "address" : "120.10.10.16"
  }
}
```

Example Responses

Status code: 201

Normal response to POST requests.

```
{
  "member" : {
    "name" : "My member",
    "weight" : 1,
    "admin_state_up" : false,
    "subnet_cidr_id" : "c09f620e-3492-4429-ac15-445d5dd9ca74",
    "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
    "address" : "120.10.10.16",
    "protocol_port" : 89,
    "id" : "1923923e-fe8a-484f-bdbc-e11559b1f48f",
    "operating_status" : "NO_MONITOR",
    "status" : [ {
      "listener_id" : "427eee03-b569-4d6c-b1f1-712032f7ec2d",
      "operating_status" : "NO_MONITOR"
    } ],
    "ip_version" : "v4"
  },
  "request_id" : "f354090d-41db-41e0-89c6-7a943ec50792"
}
```

Status Codes

Status Code	Description
201	Normal response to POST requests.

Error Codes

See **Error Codes**.

5.12.2 Querying Backend Servers

Function

This API is used to query all backend servers.

Constraints

This API has the following constraints:

- Parameters **marker**, **limit**, and **page_reverse** are used for pagination query.
- Parameters **marker** and **page_reverse** take effect only when they are used together with parameter **limit**.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/pools/{pool_id}/members

Table 5-416 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
pool_id	Yes	String	Specifies the ID of the backend server group.

Table 5-417 Query Parameters

Parameter	Mandatory	Type	Description
marker	No	String	Specifies the ID of the last record on the previous page. Note: • This parameter must be used together with **limit**. • If this parameter is not specified, the first page will be queried. • This parameter cannot be left blank or set to an invalid ID.

Parameter	Mandatory	Type	Description
limit	No	Integer	Specifies the number of records on each page. Value range: 0–2000 Default value: 2000
page_reverse	No	Boolean	Specifies whether to use reverse query. Value options: • **true**: Query the previous page. • **false** (default): Query the next page. Note: • This parameter must be used together with **limit**. • If **page_reverse** is set to **true** and you want to query the previous page, set the value of **marker** to the value of **previous_marker**.
name	No	Array of strings	Specifies the backend server name. Multiple names can be queried in the format of *name=xxx&name=xxx*.
weight	No	Array of integers	Specifies the weight of the backend server. Requests are routed to backend servers in the same backend server group based on their weights. The value ranges from **0** to **100**. The larger the weight is, the higher proportion of requests the backend server receives. If the weight is set to 0, the backend server will not accept new requests. Multiple weights can be queried in the format of *weight=xxx&weight=xxx*.

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Specifies the administrative status of the backend server. The value can be **true** or **false**. Although this parameter can be used in the APIs for creating and updating backend servers, its actual value depends on whether ECSs exist. If ECSs exist, the value is **true**. Otherwise, the value is **false**.
subnet_cidr_id	No	Array of strings	Specifies the ID of the IPv4 or IPv6 subnet where the backend server resides. Multiple IDs can be queried in the format of *subnet_cidr_id=xxx&subnet_cidr_id=xxx*.
address	No	Array of strings	Specifies the IP address bound to the backend server. Multiple IP addresses can be queried in the format of *address=xxx&address=xxx*.
protocol_port	No	Array of integers	Specifies the port used by the backend server to receive requests. Multiple ports can be queried in the format of *protocol_port=xxx&protocol_port=xxx*.
id	No	Array of strings	Specifies the backend server ID. Multiple IDs can be queried in the format of *id=xxx&id=xxx*.

Parameter	Mandatory	Type	Description
operating_status	No	Array of strings	Specifies the health status of the backend server. Value options: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group to which the backend server belongs. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist. Multiple operating statuses can be queried in the format of *operating_status=xxx&operating_status=xxx*.
enterprise_project_id	No	Array of strings	Specifies the ID of the enterprise project. • If **enterprise_project_id** is not specified, resources in all enterprise projects are queried by default. Fine-grained authorization is performed. The **elb:members:list** permission must be assigned to the user group. • If **enterprise_project_id** is specified, the value can be a specific enterprise project ID or **all_granted_eps**. If the value is a specific enterprise project ID, only resources in the enterprise project are queried. If the value is **all_granted_eps**, resources in the enterprise projects with the **elb:members:list** permission are queried. Multiple values can be queried in the format of *enterprise_project_id=xxx&enterprise_project_id=xxx*.

Parameter	Mandatory	Type	Description
ip_version	No	Array of strings	Specifies the IP version supported by the backend server. The value can be **v4** (IPv4) or **v6** (IPv6).
member_type	No	Array of strings	Specifies the type of the backend server. Value options: • **ip**: IP as backend servers • **instance**: ECSs used as backend servers Multiple values can be queried in the format of *member_type=xxx&member_type=xxx*.
instance_id	No	Array of strings	Specifies the ID of the instance associated with the backend server. If this parameter is left blank, the backend server is not an ECS. It may be an IP address. Multiple instance IDs can be queried in the format of *instance_id=xxx&instance_id=xxx*.

Request Parameters

Table 5-418 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-419 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
page_info	**PageInfo** object	Shows pagination information.
members	Array of **Member** objects	Specifies the backend servers.

Table 5-420 PageInfo

Parameter	Type	Description
previous_marker	String	Specifies the ID of the first record in the pagination query result. When **page_reverse** is set to **true**, this parameter is used together to query resources on the previous page.
next_marker	String	Specifies the ID of the last record in the pagination query result.
current_count	Integer	Specifies the number of records.

Table 5-421 Member

Parameter	Type	Description
id	String	Specifies the backend server ID. Note: The value of this parameter is not the ID of the server but an ID automatically generated for the backend server that has already been associated with the load balancer.
name	String	Specifies the backend server name. Note: The name is not an ECS name.
project_id	String	Specifies the project ID of the backend server.

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the backend server. The value can be **true** or **false**. Although this parameter can be used in the APIs for creating and updating backend servers, its actual value depends on whether ECSs exist. If ECSs exist, the value is **true**. Otherwise, the value is **false**.
subnet_cidr_id	String	Specifies the ID of the IPv4 or IPv6 subnet where the backend server resides. **neutron_subnet_id** defines IPv4 subnets, and **neutron_network_id** defines IPv6 subnets. You can query parameters **neutron_subnet_id** and **neutron_network_id** in the response by calling the API GET https://{VPC_Endpoint}/v1/{project_id}/subnets to get the IPv4 subnet ID and IPv6 subnet ID respectively. Note: • The IPv4 or IPv6 subnet must be in the same VPC as the subnet of the load balancer. • If **ip_target_enable** is set to **true**, this parameter can be left blank. In this case, IP as backend servers must use private IPv4 addresses, and the protocol of the backend server group must be TCP, UDP, TLS, HTTP, HTTPS, QUIC, or GRPC. • If **ip_target_enable** is set to **false**, this parameter must be specified.
protocol_port	Integer	Specifies the port used by the backend server to receive requests. Note: • This parameter can be left blank because it does not take effect if **any_port_enable** is set to **true** for a backend server group.

Parameter	Type	Description
weight	Integer	Specifies the weight of the backend server. Requests are routed to backend servers in the same backend server group based on their weights. The value ranges from **0** to **100**, and the default value is **1**. The larger the weight is, the higher proportion of requests the backend server receives. If the weight is set to 0, the backend server will not accept new requests. If **lb_algorithm** is set to **SOURCE_IP** or **QUIC_CID**, this parameter will not take effect.
address	String	Specifies the private IP address bound to the backend server. Note: • If **subnet_cidr_id** is left blank, **IP as a Backend** is enabled. In this case, the IP address must be an IPv4 address. • If **subnet_cidr_id** is not left blank, the IP address can be IPv4 or IPv6. It must be in the subnet specified by **subnet_cidr_id**.
ip_version	String	Specifies the IP version supported by the backend server. The value can be **v4** (IPv4) or **v6** (IPv6), depending on the value of **address** returned by the system.
operating_status	String	Specifies the health status of the backend server if **listener_id** under **status** is not specified. Value options: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group to which the backend server belongs. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist.

Parameter	Type	Description
status	Array of **MemberStatus** objects	Specifies the health status of the backend server if **listener_id** under **status** is specified. If **listener_id** under **status** is not specified, **operating_status** of **member** takes precedence.
reason	**MemberHealthCheckFailedReason** object	Specifies why health check fails.
created_at	String	Specifies the time when the backend server was added. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
updated_at	String	Specifies the time when the backend server was updated. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
member_type	String	Specifies the type of the backend server. Value options: • **ip**: IP as backend servers • **instance**: ECSs used as backend servers
instance_id	String	Specifies the ID of the instance associated with the backend server. If this parameter is left blank, the backend server is not a real device. It may be an IP address.

Table 5-422 MemberStatus

Parameter	Type	Description
listener_id	String	Specifies the listener ID.
operating_status	String	Specifies the health status of the backend server. Value options: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group to which the backend server belongs. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist.
reason	**MemberHealthCheckFailedReason** object	Specifies why health check fails.

Table 5-423 MemberHealthCheckFailedReason

Parameter	Type	Description
reason_code	String	Specifies the code of the health check failures. Value options: • **CONNECT_TIMEOUT**: The connection with the backend server times out during a health check. • **CONNECT_REFUSED**: The load balancer rejects connections with the backend server during a health check. • **CONNECT_FAILED**: The load balancer fails to establish connections with the backend server during a health check. • **CONNECT_INTERRUPT**: The load balancer is disconnected from the backend server during a health check. • **SSL_HANDSHAKE_ERROR**: The SSL handshakes with the backend server fail during a health check. • **RECV_RESPONSE_FAILED**: The load balancer fails to receive responses from the backend server during a health check. • **RECV_RESPONSE_TIMEOUT**: The load balancer does not receive responses from the backend server within the timeout duration during a health check. • **SEND_REQUEST_FAILED**: The load balancer fails to send a health check request to the backend server during a health check. • **SEND_REQUEST_TIMEOUT**: The load balancer fails to send a health check request to the backend server within the timeout duration. • **RESPONSE_FORMAT_ERROR**: The load balancer receives invalid responses from the backend server during a health check. • **RESPONSE_MISMATCH**: The response code received from the

Parameter	Type	Description
		backend server is different from the preset code.
expected_response	String	Specifies the expected HTTP status code. This parameter will take effect only when **type** is set to **HTTP**, **HTTPS**, or **GRPC**. The status code cannot be **null** if **reason_code** is **RESPONSE_MISMATCH**. Value ranges: ● A specific status code. If **type** is set to **GRPC**, the status code ranges from 0 to 99. If **type** is set to other values, the status code ranges from 200 to 599. For example, the status code can be **0** or **200**. ● A list of status codes that are separated with commas (,), for example, **200,202** or **0,1**. A maximum of five status codes are supported. ● A status code range. Different ranges are separated with commas (,), for example, **200-204,300-399** or **0-5,10-12,20-30**. A maximum of five ranges are supported.
healthcheck_response	String	Specifies the returned HTTP status code in the response. This parameter will take effect only when **type** is set to **HTTP**, **HTTPS**, or **GRPC**. The status code cannot be **null** if **reason_code** is **RESPONSE_MISMATCH**. Value range: A specific status code. If **type** is set to **GRPC**, the status code ranges from 0 to 99. If **type** is set to other values, the status code ranges from 200 to 599. For example, the status code can be **0** or **200**.

Example Requests

Querying backend servers in a given backend server group


```
GET https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/pools/36ce7086-
a496-4666-9064-5ba0e6840c75/members
```

Example Responses

Status code: 200

Successful request.

```
{
  "members" : [ {
    "name" : "quark-neutron",
    "weight" : 100,
    "admin_state_up" : false,
    "subnet_cidr_id" : "c09f620e-3492-4429-ac15-445d5dd9ca74",
    "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
    "address" : "120.10.10.2",
    "protocol_port" : 2100,
    "id" : "0aa23a52-1ac2-4a2d-8dfa-1e11cb26079d",
    "operating_status" : "NO_MONITOR",
    "ip_version" : "v4"
  }, {
    "name" : "quark-neutron",
    "weight" : 100,
    "admin_state_up" : false,
    "subnet_cidr_id" : "c09f620e-3492-4429-ac15-445d5dd9ca74",
    "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
    "address" : "120.10.10.2",
    "protocol_port" : 2101,
    "id" : "315b928b-39e4-4d5f-8e48-39e9108c1035",
    "operating_status" : "NO_MONITOR",
    "ip_version" : "v4"
  }, {
    "name" : "quark-neutron",
    "weight" : 100,
    "admin_state_up" : false,
    "subnet_cidr_id" : "27e4ab69-a5ed-46c6-921a-5212be19ce87",
    "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
    "address" : "2001:db8:a583:6a::4",
    "protocol_port" : 2101,
    "id" : "53976f72-d2aa-47f5-baf4-4906ed6b42d6",
    "operating_status" : "NO_MONITOR",
    "ip_version" : "v6"
  } ],
  "page_info" : {
    "previous_marker" : "0aa23a52-1ac2-4a2d-8dfa-1e11cb26079d",
    "current_count" : 3
  },
  "request_id" : "87e29592-7ab8-401a-9bf4-66cf6747eab9"
}
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;
```



```
public class ListMembersSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ListMembersRequest request = new ListMembersRequest();
        request.withPoolId("{pool_id}");
        try {
            ListMembersResponse response = client.listMembers(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()
```



```
    try:
        request = ListMembersRequest()
        request.pool_id = "{pool_id}"
        response = client.list_members(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListMembersRequest{}
    request.PoolId = "{pool_id}"
    response, err := client.ListMembers(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	Successful request.

Error Codes

See **Error Codes**.

5.12.3 Viewing the Details of a Backend Server

Function

This API is used to view the details of a backend server.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/pools/{pool_id}/members/{member_id}

Table 5-424 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
pool_id	Yes	String	Specifies the ID of the backend server group.
member_id	Yes	String	Specifies the backend server ID. Note: The value of this parameter is not the ID of the server but an ID automatically generated for the backend server that has already been associated with the load balancer.

Request Parameters

Table 5-425 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-426 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
member	**Member** object	Specifies the backend server.

Table 5-427 Member

Parameter	Type	Description
id	String	Specifies the backend server ID. Note: The value of this parameter is not the ID of the server but an ID automatically generated for the backend server that has already been associated with the load balancer.
name	String	Specifies the backend server name. Note: The name is not an ECS name.
project_id	String	Specifies the project ID of the backend server.
admin_state_up	Boolean	Specifies the administrative status of the backend server. The value can be **true** or **false**. Although this parameter can be used in the APIs for creating and updating backend servers, its actual value depends on whether ECSs exist. If ECSs exist, the value is **true**. Otherwise, the value is **false**.

Parameter	Type	Description
subnet_cidr_id	String	Specifies the ID of the IPv4 or IPv6 subnet where the backend server resides. **neutron_subnet_id** defines IPv4 subnets, and **neutron_network_id** defines IPv6 subnets. You can query parameters **neutron_subnet_id** and **neutron_network_id** in the response by calling the API GET https://{VPC_Endpoint}/v1/{project_id}/subnets to get the IPv4 subnet ID and IPv6 subnet ID respectively. Note: • The IPv4 or IPv6 subnet must be in the same VPC as the subnet of the load balancer. • If **ip_target_enable** is set to **true**, this parameter can be left blank. In this case, IP as backend servers must use private IPv4 addresses, and the protocol of the backend server group must be TCP, UDP, TLS, HTTP, HTTPS, QUIC, or GRPC. • If **ip_target_enable** is set to **false**, this parameter must be specified.
protocol_port	Integer	Specifies the port used by the backend server to receive requests. Note: • This parameter can be left blank because it does not take effect if **any_port_enable** is set to **true** for a backend server group.
weight	Integer	Specifies the weight of the backend server. Requests are routed to backend servers in the same backend server group based on their weights. The value ranges from **0** to **100**, and the default value is **1**. The larger the weight is, the higher proportion of requests the backend server receives. If the weight is set to 0, the backend server will not accept new requests. If **lb_algorithm** is set to **SOURCE_IP** or **QUIC_CID**, this parameter will not take effect.

Parameter	Type	Description
address	String	Specifies the private IP address bound to the backend server. Note: • If **subnet_cidr_id** is left blank, **IP as a Backend** is enabled. In this case, the IP address must be an IPv4 address. • If **subnet_cidr_id** is not left blank, the IP address can be IPv4 or IPv6. It must be in the subnet specified by **subnet_cidr_id**.
ip_version	String	Specifies the IP version supported by the backend server. The value can be **v4** (IPv4) or **v6** (IPv6), depending on the value of **address** returned by the system.
operating_status	String	Specifies the health status of the backend server if **listener_id** under **status** is not specified. Value options: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group to which the backend server belongs. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist.
status	Array of **MemberStatus** objects	Specifies the health status of the backend server if **listener_id** under **status** is specified. If **listener_id** under **status** is not specified, **operating_status** of **member** takes precedence.
reason	**MemberHealthCheckFailedReason** object	Specifies why health check fails.

Parameter	Type	Description
created_at	String	Specifies the time when the backend server was added. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
updated_at	String	Specifies the time when the backend server was updated. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
member_type	String	Specifies the type of the backend server. Value options: • **ip**: IP as backend servers • **instance**: ECSs used as backend servers
instance_id	String	Specifies the ID of the instance associated with the backend server. If this parameter is left blank, the backend server is not a real device. It may be an IP address.

Table 5-428 MemberStatus

Parameter	Type	Description
listener_id	String	Specifies the listener ID.

Parameter	Type	Description
operating_status	String	Specifies the health status of the backend server. Value options: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group to which the backend server belongs. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist.
reason	**MemberHealthCheckFailedReason** object	Specifies why health check fails.

Table 5-429 MemberHealthCheckFailedReason

Parameter	Type	Description
reason_code	String	Specifies the code of the health check failures. Value options: • **CONNECT_TIMEOUT**: The connection with the backend server times out during a health check. • **CONNECT_REFUSED**: The load balancer rejects connections with the backend server during a health check. • **CONNECT_FAILED**: The load balancer fails to establish connections with the backend server during a health check. • **CONNECT_INTERRUPT**: The load balancer is disconnected from the backend server during a health check. • **SSL_HANDSHAKE_ERROR**: The SSL handshakes with the backend server fail during a health check. • **RECV_RESPONSE_FAILED**: The load balancer fails to receive responses from the backend server during a health check. • **RECV_RESPONSE_TIMEOUT**: The load balancer does not receive responses from the backend server within the timeout duration during a health check. • **SEND_REQUEST_FAILED**: The load balancer fails to send a health check request to the backend server during a health check. • **SEND_REQUEST_TIMEOUT**: The load balancer fails to send a health check request to the backend server within the timeout duration. • **RESPONSE_FORMAT_ERROR**: The load balancer receives invalid responses from the backend server during a health check. • **RESPONSE_MISMATCH**: The response code received from the

Parameter	Type	Description
		backend server is different from the preset code.
expected_response	String	Specifies the expected HTTP status code. This parameter will take effect only when **type** is set to **HTTP**, **HTTPS**, or **GRPC**. The status code cannot be **null** if **reason_code** is **RESPONSE_MISMATCH**. Value ranges: • A specific status code. If **type** is set to **GRPC**, the status code ranges from 0 to 99. If **type** is set to other values, the status code ranges from 200 to 599. For example, the status code can be **0** or **200**. • A list of status codes that are separated with commas (,), for example, **200,202** or **0,1**. A maximum of five status codes are supported. • A status code range. Different ranges are separated with commas (,), for example, **200-204,300-399** or **0-5,10-12,20-30**. A maximum of five ranges are supported.
healthcheck_response	String	Specifies the returned HTTP status code in the response. This parameter will take effect only when **type** is set to **HTTP**, **HTTPS**, or **GRPC**. The status code cannot be **null** if **reason_code** is **RESPONSE_MISMATCH**. Value range: A specific status code. If **type** is set to **GRPC**, the status code ranges from 0 to 99. If **type** is set to other values, the status code ranges from 200 to 599. For example, the status code can be **0** or **200**.

Example Requests

Querying the details of a backend server


```
GET https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/pools/36ce7086-
a496-4666-9064-5ba0e6840c75/members/1923923e-fe8a-484f-bdbc-e11559b1f48f
```

Example Responses

Status code: 200

Successful request.

```
{
  "member" : {
    "name" : "My member",
    "weight" : 10,
    "admin_state_up" : false,
    "subnet_cidr_id" : "c09f620e-3492-4429-ac15-445d5dd9ca74",
    "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
    "address" : "120.10.10.16",
    "protocol_port" : 89,
    "id" : "1923923e-fe8a-484f-bdbc-e11559b1f48f",
    "operating_status" : "NO_MONITOR",
    "ip_version" : "v4"
  },
  "request_id" : "45688823-45f1-40cd-9d24-e51a9574a45b"
}
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ShowMemberSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowMemberRequest request = new ShowMemberRequest();
        request.withPoolId("{pool_id}");
        request.withMemberId("{member_id}");
```



```
        try {
            ShowMemberResponse response = client.showMember(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowMemberRequest()
        request.pool_id = "{pool_id}"
        request.member_id = "{member_id}"
        response = client.show_member(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowMemberRequest{}
    request.PoolId = "{pool_id}"
    request.MemberId = "{member_id}"
    response, err := client.ShowMember(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	Successful request.

Error Codes

See **Error Codes**.

5.12.4 Updating a Backend Server

Function

This API is used to update a backend server.

Constraints

If the provisioning status of the associated load balancer is not **ACTIVE**, the backend server cannot be updated.

Calling Method

For details, see **Calling APIs**.

URI

PUT /v3/{project_id}/elb/pools/{pool_id}/members/{member_id}

Table 5-430 Path Parameters

Parameter	Mandatory	Type	Description
member_id	Yes	String	Specifies the backend server ID. Note: The value of this parameter is not the ID of the server but an ID automatically generated for the backend server that has already been associated with the load balancer.
pool_id	Yes	String	Specifies the ID of the backend server group.
project_id	Yes	String	Specifies the project ID.

Request Parameters

Table 5-431 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Table 5-432 Request body parameters

Parameter	Mandatory	Type	Description
member	Yes	**UpdateMemberOption** object	Specifies the backend server.

Table 5-433 UpdateMemberOption

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Specifies the administrative status of the backend server. The value can be **true** or **false**. Although this parameter can be used in the APIs for creating and updating backend servers, its actual value depends on whether ECSs exist. If ECSs exist, the value is **true**. Otherwise, the value is **false**. Please do not specify this parameter.
name	No	String	Specifies the backend server name.
weight	No	Integer	Specifies the weight of the backend server. Requests are routed to backend servers in the same backend server group based on their weights. The value ranges from **0** to **100**, and the default value is **1**. The larger the weight is, the higher proportion of requests the backend server receives. If the weight is set to 0, the backend server will not accept new requests. If **lb_algorithm** is set to **SOURCE_IP** or **QUIC_CID**, this parameter will not take effect.
protocol_port	No	Integer	Specifies the port used by the backend server to receive requests. **NOTE** This parameter cannot be updated if **any_port_enable** is set to **true** for a backend server group.

Response Parameters

Status code: 200

Table 5-434 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
member	**Member** object	Specifies the backend server.

Table 5-435 Member

Parameter	Type	Description
id	String	Specifies the backend server ID. Note: The value of this parameter is not the ID of the server but an ID automatically generated for the backend server that has already been associated with the load balancer.
name	String	Specifies the backend server name. Note: The name is not an ECS name.
project_id	String	Specifies the project ID of the backend server.
admin_state_up	Boolean	Specifies the administrative status of the backend server. The value can be **true** or **false**. Although this parameter can be used in the APIs for creating and updating backend servers, its actual value depends on whether ECSs exist. If ECSs exist, the value is **true**. Otherwise, the value is **false**.

Parameter	Type	Description
subnet_cidr_id	String	Specifies the ID of the IPv4 or IPv6 subnet where the backend server resides. **neutron_subnet_id** defines IPv4 subnets, and **neutron_network_id** defines IPv6 subnets. You can query parameters **neutron_subnet_id** and **neutron_network_id** in the response by calling the API GET https://{VPC_Endpoint}/v1/{project_id}/subnets to get the IPv4 subnet ID and IPv6 subnet ID respectively. Note: • The IPv4 or IPv6 subnet must be in the same VPC as the subnet of the load balancer. • If **ip_target_enable** is set to **true**, this parameter can be left blank. In this case, IP as backend servers must use private IPv4 addresses, and the protocol of the backend server group must be TCP, UDP, TLS, HTTP, HTTPS, QUIC, or GRPC. • If **ip_target_enable** is set to **false**, this parameter must be specified.
protocol_port	Integer	Specifies the port used by the backend server to receive requests. Note: • This parameter can be left blank because it does not take effect if **any_port_enable** is set to **true** for a backend server group.
weight	Integer	Specifies the weight of the backend server. Requests are routed to backend servers in the same backend server group based on their weights. The value ranges from **0** to **100**, and the default value is **1**. The larger the weight is, the higher proportion of requests the backend server receives. If the weight is set to 0, the backend server will not accept new requests. If **lb_algorithm** is set to **SOURCE_IP** or **QUIC_CID**, this parameter will not take effect.

Parameter	Type	Description
address	String	Specifies the private IP address bound to the backend server. Note: • If **subnet_cidr_id** is left blank, **IP as a Backend** is enabled. In this case, the IP address must be an IPv4 address. • If **subnet_cidr_id** is not left blank, the IP address can be IPv4 or IPv6. It must be in the subnet specified by **subnet_cidr_id**.
ip_version	String	Specifies the IP version supported by the backend server. The value can be **v4** (IPv4) or **v6** (IPv6), depending on the value of **address** returned by the system.
operating_status	String	Specifies the health status of the backend server if **listener_id** under **status** is not specified. Value options: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group to which the backend server belongs. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist.
status	Array of **MemberStatus** objects	Specifies the health status of the backend server if **listener_id** under **status** is specified. If **listener_id** under **status** is not specified, **operating_status** of **member** takes precedence.
reason	**MemberHealthCheckFailedReason** object	Specifies why health check fails.

Parameter	Type	Description
created_at	String	Specifies the time when the backend server was added. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
updated_at	String	Specifies the time when the backend server was updated. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
member_type	String	Specifies the type of the backend server. Value options: • **ip**: IP as backend servers • **instance**: ECSs used as backend servers
instance_id	String	Specifies the ID of the instance associated with the backend server. If this parameter is left blank, the backend server is not a real device. It may be an IP address.

Table 5-436 MemberStatus

Parameter	Type	Description
listener_id	String	Specifies the listener ID.

Parameter	Type	Description
operating_status	String	Specifies the health status of the backend server. Value options: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group to which the backend server belongs. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist.
reason	**MemberHealthCheckFailedReason** object	Specifies why health check fails.

Table 5-437 MemberHealthCheckFailedReason

Parameter	Type	Description
reason_code	String	Specifies the code of the health check failures. Value options: • **CONNECT_TIMEOUT**: The connection with the backend server times out during a health check. • **CONNECT_REFUSED**: The load balancer rejects connections with the backend server during a health check. • **CONNECT_FAILED**: The load balancer fails to establish connections with the backend server during a health check. • **CONNECT_INTERRUPT**: The load balancer is disconnected from the backend server during a health check. • **SSL_HANDSHAKE_ERROR**: The SSL handshakes with the backend server fail during a health check. • **RECV_RESPONSE_FAILED**: The load balancer fails to receive responses from the backend server during a health check. • **RECV_RESPONSE_TIMEOUT**: The load balancer does not receive responses from the backend server within the timeout duration during a health check. • **SEND_REQUEST_FAILED**: The load balancer fails to send a health check request to the backend server during a health check. • **SEND_REQUEST_TIMEOUT**: The load balancer fails to send a health check request to the backend server within the timeout duration. • **RESPONSE_FORMAT_ERROR**: The load balancer receives invalid responses from the backend server during a health check. • **RESPONSE_MISMATCH**: The response code received from the

Parameter	Type	Description
		backend server is different from the preset code.
expected_response	String	Specifies the expected HTTP status code. This parameter will take effect only when **type** is set to **HTTP**, **HTTPS**, or **GRPC**. The status code cannot be **null** if **reason_code** is **RESPONSE_MISMATCH**. Value ranges: • A specific status code. If **type** is set to **GRPC**, the status code ranges from 0 to 99. If **type** is set to other values, the status code ranges from 200 to 599. For example, the status code can be **0** or **200**. • A list of status codes that are separated with commas (,), for example, **200,202** or **0,1**. A maximum of five status codes are supported. • A status code range. Different ranges are separated with commas (,), for example, **200-204,300-399** or **0-5,10-12,20-30**. A maximum of five ranges are supported.
healthcheck_response	String	Specifies the returned HTTP status code in the response. This parameter will take effect only when **type** is set to **HTTP**, **HTTPS**, or **GRPC**. The status code cannot be **null** if **reason_code** is **RESPONSE_MISMATCH**. Value range: A specific status code. If **type** is set to **GRPC**, the status code ranges from 0 to 99. If **type** is set to other values, the status code ranges from 200 to 599. For example, the status code can be **0** or **200**.

Example Requests

Changing the weight of a backend server


```
PUT https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/pools/36ce7086-
a496-4666-9064-5ba0e6840c75/members/1923923e-fe8a-484f-bdbc-e11559b1f48f

{
  "member" : {
    "name" : "My member",
    "weight" : 10
  }
}
```

Example Responses

Status code: 200

Successful request.

```
{
  "member" : {
    "name" : "My member",
    "weight" : 10,
    "admin_state_up" : false,
    "subnet_cidr_id" : "c09f620e-3492-4429-ac15-445d5dd9ca74",
    "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
    "address" : "120.10.10.16",
    "protocol_port" : 89,
    "id" : "1923923e-fe8a-484f-bdbc-e11559b1f48f",
    "operating_status" : "NO_MONITOR",
    "ip_version" : "v4"
  },
  "request_id" : "e7b569d4-15ad-494d-9dd9-8cd740eef8f6"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Changing the weight of a backend server

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class UpdateMemberSolution {

    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);

    ElbClient client = ElbClient.newBuilder()
            .withCredential(auth)
            .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
            .build();
    UpdateMemberRequest request = new UpdateMemberRequest();
    request.withMemberId("{member_id}");
    request.withPoolId("{pool_id}");
    UpdateMemberRequestBody body = new UpdateMemberRequestBody();
    UpdateMemberOption memberbody = new UpdateMemberOption();
    memberbody.withName("My member")
        .withWeight(10);
    body.withMember(memberbody);
    request.withBody(body);
    try {
        UpdateMemberResponse response = client.updateMember(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

Changing the weight of a backend server

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdateMemberRequest()
        request.member_id = "{member_id}"
        request.pool_id = "{pool_id}"
        memberbody = UpdateMemberOption(
            name="My member",
            weight=10
```



```
        )
        request.body = UpdateMemberRequestBody(
            member=memberbody
        )
        response = client.update_member(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

Changing the weight of a backend server

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdateMemberRequest{}
    request.MemberId = "{member_id}"
    request.PoolId = "{pool_id}"
    nameMember:= "My member"
    weightMember:= int32(10)
    memberbody := &model.UpdateMemberOption{
        Name: &nameMember,
        Weight: &weightMember,
    }
    request.Body = &model.UpdateMemberRequestBody{
        Member: memberbody,
    }
    response, err := client.UpdateMember(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	Successful request.

Error Codes

See **Error Codes**.

5.12.5 Removing a Backend Server

Function

This API is used to remove a backend server.

Constraints

After you remove a backend server, new connections to this server will not be established. However, persistent connections that have been established will be maintained.

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v3/{project_id}/elb/pools/{pool_id}/members/{member_id}

Table 5-438 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
pool_id	Yes	String	Specifies the ID of the backend server group.

Parameter	Mandatory	Type	Description
member_id	Yes	String	Specifies the backend server ID. Note: The value of this parameter is not the ID of the server but an ID automatically generated for the backend server that has already been associated with the load balancer. You can obtain the server ID by calling the API for querying the backend servers.

Request Parameters

Table 5-439 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

None

Example Requests

Deleting a given backend server

```
DELETE https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/pools/36ce7086-a496-4666-9064-5ba0e6840c75/members/1923923e-fe8a-484f-bdbc-e11559b1f48f
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class DeleteMemberSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteMemberRequest request = new DeleteMemberRequest();
        request.withPoolId("{pool_id}");
        request.withMemberId("{member_id}");
        try {
            DeleteMemberResponse response = client.deleteMember(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteMemberRequest()
        request.pool_id = "{pool_id}"
        request.member_id = "{member_id}"
        response = client.delete_member(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteMemberRequest{}
    request.PoolId = "{pool_id}"
    request.MemberId = "{member_id}"
    response, err := client.DeleteMember(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	Successful request.

Error Codes

See **Error Codes**.

5.12.6 Querying Backend Servers

Function

This API is used to query the backend servers under the current project.

Constraints

This API has the following constraints:

- Parameters **marker**, **limit**, and **page_reverse** are used for pagination query.
- Parameters **marker** and **page_reverse** take effect only when they are used together with parameter **limit**.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/members

Table 5-440 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Table 5-441 Query Parameters

Parameter	Mandatory	Type	Description
marker	No	String	Specifies the ID of the last record on the previous page. Note: • This parameter must be used together with **limit**. • If this parameter is not specified, the first page will be queried. • This parameter cannot be left blank or set to an invalid ID.
limit	No	Integer	Specifies the number of records on each page. Value range: 0–2000 Default value: 2000
page_reverse	No	Boolean	Specifies whether to use reverse query. Value options: • **true**: Query the previous page. • **false** (default): Query the next page. Note: • This parameter must be used together with **limit**. • If **page_reverse** is set to **true** and you want to query the previous page, set the value of **marker** to the value of **previous_marker**.
name	No	Array of strings	Specifies the backend server name. Multiple names can be queried in the format of *name=xxx&name=xxx*.

Parameter	Mandatory	Type	Description
weight	No	Array of integers	Specifies the weight of the backend server. Requests are routed to backend servers in the same backend server group based on their weights. If the weight is **0**, the backend server will not accept new requests. This parameter is invalid when **lb_algorithm** is set to **SOURCE_IP** for the backend server group that contains the backend server. Multiple weights can be queried in the format of *weight=xxx&weight=xxx*.
admin_state_up	No	Boolean	Specifies the administrative status of the backend server. The value can be **true** or **false**. Although this parameter can be used in the APIs for creating and updating backend servers, its actual value depends on whether ECSs exist. If ECSs exist, the value is **true**. Otherwise, the value is **false**.
subnet_cidr_id	No	Array of strings	Specifies the ID of the subnet where the backend server works. This subnet must be in the same VPC as the subnet of the load balancer with which the backend server is associated. Only IPv4 subnets are supported. Multiple IDs can be queried in the format of *subnet_cidr_id=xxx&subnet_cidr_id=xxx*.

Parameter	Mandatory	Type	Description
address	No	Array of strings	Specifies the IP address of the backend server. This address must be in the subnet specified by **subnet_cidr_id**, for example, 192.168.3.11. The IP address can only be the IP address of the primary NIC. Multiple IP addresses can be queried in the format of *address=xxx&address=xxx*.
protocol_port	No	Array of integers	Specifies the port used by the backend servers. Multiple ports can be queried in the format of *protocol_port=xxx&protocol_port=xxx*.
id	No	Array of strings	Specifies the backend server ID. Multiple IDs can be queried in the format of *id=xxx&id=xxx*.
operating_status	No	Array of strings	Specifies the operating status of the backend server. Value options: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group to which the backend server belongs. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist. Multiple statuses can be queried in the format of *operating_status=xxx&operating_status=xxx*.

Parameter	Mandatory	Type	Description
enterprise_project_id	No	Array of strings	Specifies the ID of the enterprise project. • If **enterprise_project_id** is not specified, resources in all enterprise projects are queried by default. Fine-grained authorization is performed. The **elb:members:list** permission must be assigned to the user group. • If **enterprise_project_id** is specified, the value can be a specific enterprise project ID or **all_granted_eps**. If the value is a specific enterprise project ID, only resources in the enterprise project are queried. If the value is **all_granted_eps**, resources in the enterprise projects with the **elb:members:list** permission are queried. Multiple values can be queried in the format of *enterprise_project_id=xxx&enterprise_project_id=xxx*.
ip_version	No	Array of strings	Specifies the IP address version supported by the backend server group. The value can be **v4** or **v6**. Multiple versions can be queried in the format of *ip_version=xxx&ip_version=xxx*.
pool_id	No	Array of strings	Specifies the ID of the backend server group to which the backend server belongs. Multiple IDs can be queried in the format of *pool_id=xxx&pool_id=xxx*.

Parameter	Mandatory	Type	Description
loadbalancer_id	No	Array of strings	Specifies the ID of the load balancer with which the load balancer is associated. Multiple IDs can be queried in the format of *loadbalancer_id=xxx&loadbalancer_id=xxx*.

Request Parameters

Table 5-442 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-443 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
page_info	**PageInfo** object	Pagination information.
members	Array of **MemberInfo** objects	Specifies the backend servers.

Table 5-444 PageInfo

Parameter	Type	Description
previous_marker	String	Specifies the ID of the first record in the pagination query result. When **page_reverse** is set to **true**, this parameter is used together to query resources on the previous page.

Parameter	Type	Description
next_marker	String	Specifies the ID of the last record in the pagination query result.
current_count	Integer	Specifies the number of records.

Table 5-445 MemberInfo

Parameter	Type	Description
id	String	Specifies the backend server ID. Note: The value of this parameter is not the ID of the server but an ID automatically generated for the backend server that has already been associated with the load balancer.
name	String	Specifies the backend server name. Note: The name is not an ECS name.
project_id	String	Specifies the ID of the project where the backend server is used.
pool_id	String	Specifies the ID of the backend server group to which the backend server belongs. This parameter is unsupported. Please do not use it.
admin_state_up	Boolean	Specifies the administrative status of the backend server. The value can be **true** or **false**. Although this parameter can be used in the APIs for creating and updating backend servers, its actual value depends on whether ECSs exist. If ECSs exist, the value is **true**. Otherwise, the value is **false**.

Parameter	Type	Description
subnet_cidr_id	String	Specifies the ID of the IPv4 or IPv6 subnet where the backend server resides. **neutron_subnet_id** defines IPv4 subnets, and **neutron_network_id** defines IPv6 subnets. You can query parameters **neutron_subnet_id** and **neutron_network_id** in the response by calling the API GET https://{VPC_Endpoint}/v1/{project_id}/subnets to get the IPv4 subnet ID and IPv6 subnet ID respectively. Note: • The IPv4 or IPv6 subnet must be in the same VPC as the subnet of the load balancer. • If **ip_target_enable** is set to **true**, this parameter can be left blank. In this case, IP as backend servers must use private IPv4 addresses, and the protocol of the backend server group must be TCP, UDP, TLS, HTTP, HTTPS, QUIC, or GRPC. • If **ip_target_enable** is set to **false**, this parameter must be specified.
protocol_port	Integer	Specifies the port used by the backend server to receive requests. Note: • This parameter can be left blank because it does not take effect if **any_port_enable** is set to **true** for a backend server group.
weight	Integer	Specifies the weight of the backend server. Requests are routed to backend servers in the same backend server group based on their weights. The value ranges from **0** to **100**, and the default value is **1**. The larger the weight is, the higher proportion of requests the backend server receives. If the weight is set to 0, the backend server will not accept new requests. If **lb_algorithm** is set to **SOURCE_IP** or **QUIC_CID**, this parameter will not take effect.

Parameter	Type	Description
address	String	Specifies the private IP address bound to the backend server. Note: • If **subnet_cidr_id** is left blank, **IP as a Backend** is enabled. In this case, the IP address must be an IPv4 address. • If **subnet_cidr_id** is not left blank, the IP address can be IPv4 or IPv6. It must be in the subnet specified by **subnet_cidr_id**.
ip_version	String	Specifies the IP version supported by the backend server. The value can be **v4** (IPv4) or **v6** (IPv6), depending on the value of **address** returned by the system.
device_owner	String	Specifies whether the backend server is associated with an ECS. • If this parameter is left blank, the backend server is not associated with an ECS. • If the value is **compute:{az_name}**, the backend server is associated with an ECS. **{az_name}** indicates the AZ where the ECS resides. • If the value is **compute:subeni**, supplementary network interfaces are added as backend servers. This parameter is unsupported. Please do not use it.
device_id	String	Specifies the ID of the ECS with which the backend server is associated. If this parameter is left blank, the backend server is not associated with an ECS. This parameter is unsupported. Please do not use it.

Parameter	Type	Description
operating_status	String	Specifies the health status of the backend server if **listener_id** under **status** is not specified. Value options: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group to which the backend server belongs. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist.
status	Array of **MemberStatus** objects	Specifies the health status of the backend server if **listener_id** under **status** is specified. If **listener_id** under **status** is not specified, **operating_status** of **member** takes precedence.
loadbalancer_id	String	Specifies the ID of the load balancer with which the backend server is associated. This parameter is unsupported. Please do not use it.
loadbalancers	Array of **ResourceID** objects	Specifies the IDs of the load balancers associated with the backend server. This parameter is unsupported. Please do not use it.
created_at	String	Specifies the time when a backend server was added. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.

Parameter	Type	Description
updated_at	String	Specifies the time when a backend server was updated. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
member_type	String	Specifies the type of the backend server. Value options: • **ip**: IP addresses added as backend servers • **instance**: ECSs used as backend servers
instance_id	String	Specifies the ID of the instance associated with the backend server. If this parameter is left blank, the backend server is not a real device. It may be an IP address.
reason	**MemberHealthCheckFailedReason** object	Specifies why health check fails.

Table 5-446 MemberStatus

Parameter	Type	Description
listener_id	String	Specifies the listener ID.
operating_status	String	Specifies the health status of the backend server. Value options: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group to which the backend server belongs. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist.

Parameter	Type	Description
reason	**MemberHealthCheckFailedReason** object	Specifies why health check fails.

Table 5-447 ResourceID

Parameter	Type	Description
id	String	Specifies the resource ID.

Table 5-448 MemberHealthCheckFailedReason

Parameter	Type	Description
reason_code	String	Specifies the code of the health check failures. Value options: • **CONNECT_TIMEOUT**: The connection with the backend server times out during a health check. • **CONNECT_REFUSED**: The load balancer rejects connections with the backend server during a health check. • **CONNECT_FAILED**: The load balancer fails to establish connections with the backend server during a health check. • **CONNECT_INTERRUPT**: The load balancer is disconnected from the backend server during a health check. • **SSL_HANDSHAKE_ERROR**: The SSL handshakes with the backend server fail during a health check. • **RECV_RESPONSE_FAILED**: The load balancer fails to receive responses from the backend server during a health check. • **RECV_RESPONSE_TIMEOUT**: The load balancer does not receive responses from the backend server within the timeout duration during a health check. • **SEND_REQUEST_FAILED**: The load balancer fails to send a health check request to the backend server during a health check. • **SEND_REQUEST_TIMEOUT**: The load balancer fails to send a health check request to the backend server within the timeout duration. • **RESPONSE_FORMAT_ERROR**: The load balancer receives invalid responses from the backend server during a health check. • **RESPONSE_MISMATCH**: The response code received from the

Parameter	Type	Description
		backend server is different from the preset code.
expected_response	String	Specifies the expected HTTP status code. This parameter will take effect only when **type** is set to **HTTP**, **HTTPS**, or **GRPC**. The status code cannot be **null** if **reason_code** is **RESPONSE_MISMATCH**. Value ranges: ● A specific status code. If **type** is set to **GRPC**, the status code ranges from 0 to 99. If **type** is set to other values, the status code ranges from 200 to 599. For example, the status code can be **0** or **200**. ● A list of status codes that are separated with commas (,), for example, **200,202** or **0,1**. A maximum of five status codes are supported. ● A status code range. Different ranges are separated with commas (,), for example, **200-204,300-399** or **0-5,10-12,20-30**. A maximum of five ranges are supported.
healthcheck_response	String	Specifies the returned HTTP status code in the response. This parameter will take effect only when **type** is set to **HTTP**, **HTTPS**, or **GRPC**. The status code cannot be **null** if **reason_code** is **RESPONSE_MISMATCH**. Value range: A specific status code. If **type** is set to **GRPC**, the status code ranges from 0 to 99. If **type** is set to other values, the status code ranges from 200 to 599. For example, the status code can be **0** or **200**.

Example Requests

Querying all backend servers under the current project


```
GET https://{ELB_Endpoint}/v3/7a9941d34fc1497d8d0797429ecfd354/elb/members
```

Example Responses

Status code: 200

Successful request.


```
{
  "request_id" : "9bd54b2c-b6c6-4635-9495-dd89bdd917ad",
  "members" : [ {
    "name" : "member-1",
    "weight" : 1,
    "admin_state_up" : true,
    "project_id" : "86f9bb15ce80442680229fcd4dc96582",
    "address" : "192.168.0.157",
    "protocol_port" : 80,
    "id" : "f5e20309-c79c-470c-b59c-3c8378792897",
    "operating_status" : "ONLINE",
    "status" : [ {
      "listener_id" : "0663b12d-4a8f-4ee1-8ba2-dd09f2c92ef7",
      "operating_status" : "ONLINE"
    }, {
      "listener_id" : "19ac6a54-336f-44ce-9679-50c4f56e9407",
      "operating_status" : "ONLINE"
    } ],
    "instance_id" : "39b7d471-fbb4-4e6d-ac81-635b4415a27f",
    "device_id" : "39b7d471-fbb4-4e6d-ac81-635b4415a27f",
    "device_owner" : "compute:cn-southwest-242a",
    "member_type" : "instance",
    "created_at" : "2023-05-04T06:55:33Z",
    "updated_at" : "2023-05-08T01:34:02Z",
    "loadbalancer_id" : "9eafbe79-4d48-46f6-95e6-0bc3da57b96d",
    "loadbalancers" : [ {
      "id" : "9eafbe79-4d48-46f6-95e6-0bc3da57b96d"
    } ],
    "pool_id" : "46cd9381-3d99-4e32-b799-efaf5c274586",
    "ip_version" : "v4",
    "subnet_cidr_id" : "1aee2ab8-f238-4c26-8659-2a7a0c201d0a"
  }, {
    "name" : "member-2",
    "admin_state_up" : true,
    "project_id" : "86f9bb15ce80442680229fcd4dc96582",
    "address" : "192.168.0.157",
    "protocol_port" : 80,
    "id" : "f834d6c6-b376-4031-931e-57cb36bca4a8",
    "operating_status" : "OFFLINE",
    "status" : [ ],
    "instance_id" : "39b7d471-fbb4-4e6d-ac81-635b4415a27f",
    "device_id" : "39b7d471-fbb4-4e6d-ac81-635b4415a27f",
    "device_owner" : "compute:cn-southwest-242a",
    "member_type" : "instance",
    "created_at" : "2023-05-04T12:46:55Z",
    "updated_at" : "2023-05-05T03:56:40Z",
    "loadbalancers" : [ ],
    "pool_id" : "d17d07db-5bab-4a15-aa6f-8561af133ca7",
    "ip_version" : "v4",
    "subnet_cidr_id" : "1aee2ab8-f238-4c26-8659-2a7a0c201d0a"
  } ],
  "page_info" : {
    "next_marker" : "fb1ce58f-2525-4bd9-9606-10851533bd22",
    "previous_marker" : "fb19f821-5d5f-4d72-b11c-503e874d3915",
    "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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ListAllMembersSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ListAllMembersRequest request = new ListAllMembersRequest();
        try {
            ListAllMembersResponse response = client.listAllMembers(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListAllMembersRequest()
        response = client.list_all_members(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListAllMembersRequest{}
    response, err := client.ListAllMembers(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	Successful request.

Error Codes

See **Error Codes**.

5.12.7 Batch Adding Backend Servers

Function

This API is used to add backend servers to the specified backend server group in batches. You can add up to 200 backend servers at a time to a backend server group.

Calling Method

For details, see **Calling APIs**.

URI

POST /v3/{project_id}/elb/pools/{pool_id}/members/batch-add

Table 5-449 Path Parameters

Parameter	Mandatory	Type	Description
pool_id	Yes	String	Specifies the ID of the backend server group.
project_id	Yes	String	Specifies the project ID.

Request Parameters

Table 5-450 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Table 5-451 Request body parameters

Parameter	Mandatory	Type	Description
members	Yes	Array of **BatchCreateMembersOption** objects	Specifies the backend server.

Table 5-452 BatchCreateMembersOption

Parameter	Mandatory	Type	Description
name	No	String	Specifies the backend server name.
address	Yes	String	Specifies the IP address of the backend server. This IP address must be in the subnet specified by **subnet_cidr_id**, for example, 192.168.3.11. If **subnet_cidr_id** is left blank, a server of **IP as a Backend** can be added. In this case, the address must be an IPv4 address.
protocol_port	Yes	Integer	Specifies the port used by the backend server to receive requests. Note: • This parameter can be left blank because it does not take effect if **any_port_enable** is set to **true** for a backend server group.

Parameter	Mandatory	Type	Description
subnet_cidr_id	No	String	Specifies the ID of the IPv4 or IPv6 subnet where the backend server resides. **neutron_subnet_id** defines IPv4 subnets, and **neutron_network_id** defines IPv6 subnets. You can query parameters **neutron_subnet_id** and **neutron_network_id** in the response by calling the API GET https://{VPC_Endpoint}/v1/{project_id}/subnets to get the IPv4 subnet ID and IPv6 subnet ID respectively. Note: • The IPv4 or IPv6 subnet must be in the same VPC as the subnet of the load balancer. • If **ip_target_enable** is set to **true**, this parameter can be left blank. In this case, IP as backend servers must use private IPv4 addresses, and the protocol of the backend server group must be TCP, UDP, TLS, HTTP, HTTPS, QUIC, or GRPC. • If **ip_target_enable** is set to **false**, this parameter must be specified.

Parameter	Mandatory	Type	Description
weight	No	Integer	Specifies the weight of the backend server. Requests are routed to backend servers in the same backend server group based on their weights. The value ranges from **0** to **100**, and the default value is **1**. The larger the weight is, the higher proportion of requests the backend server receives. If the weight is set to 0, the backend server will not accept new requests. If **lb_algorithm** is set to **SOURCE_IP** or **QUIC_CID**, this parameter will not take effect.

Response Parameters

Status code: 201

Table 5-453 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
members	Array of **BatchMember** objects	Specifies the backend servers.

Table 5-454 BatchMember

Parameter	Type	Description
id	String	Specifies the backend server ID. Note: The value of this parameter is not the ID of the server but an ID automatically generated for the backend server that has already been associated with the load balancer.
name	String	Specifies the backend server name.

Parameter	Type	Description
project_id	String	Specifies the ID of the project that the backend server is associated with.
admin_state_up	Boolean	Specifies the administrative status of the backend server. The value can be **true** or **false**. Although this parameter can be used in the APIs for creating and updating backend servers, its actual value depends on whether ECSs exist. If ECSs exist, the value is **true**. Otherwise, the value is **false**.
subnet_cidr_id	String	Specifies the ID of the IPv4 or IPv6 subnet where the backend server resides. **neutron_subnet_id** defines IPv4 subnets, and **neutron_network_id** defines IPv6 subnets. You can query parameters **neutron_subnet_id** and **neutron_network_id** in the response by calling the API GET https://{VPC_Endpoint}/v1/{project_id}/subnets to get the IPv4 subnet ID and IPv6 subnet ID respectively. Note: • The IPv4 or IPv6 subnet must be in the same VPC as the subnet of the load balancer. • If **ip_target_enable** is set to **true**, this parameter can be left blank. In this case, IP as backend servers must use private IPv4 addresses, and the protocol of the backend server group must be TCP, UDP, TLS, HTTP, HTTPS, QUIC, or GRPC. • If **ip_target_enable** is set to **false**, this parameter must be specified.
protocol_port	Integer	Specifies the port used by the backend server to receive requests. Note: • This parameter can be left blank because it does not take effect if **any_port_enable** is set to **true** for a backend server group.

Parameter	Type	Description
weight	Integer	Specifies the weight of the backend server. Requests are routed to backend servers in the same backend server group based on their weights. The value ranges from **0** to **100**, and the default value is **1**. The larger the weight is, the higher proportion of requests the backend server receives. If the weight is set to 0, the backend server will not accept new requests. If **lb_algorithm** is set to **SOURCE_IP** or **QUIC_CID**, this parameter will not take effect.
address	String	Specifies the private IP address bound to the backend server. Note: • If **subnet_cidr_id** is left blank, **IP as a Backend** is enabled. In this case, the IP address must be an IPv4 address. • If **subnet_cidr_id** is not left blank, the IP address can be IPv4 or IPv6. It must be in the subnet specified by **subnet_cidr_id**.
operating_status	String	Specifies the health status of the backend server. Value options: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group to which the backend server belongs. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist.
reason	**MemberHealthCheckFailedReason** object	Specifies why health check fails.
status	Array of **MemberStatus** objects	Specifies the health status of the backend server if **listener_id** under **status** is specified. If **listener_id** under **status** is not specified, **operating_status** of **member** takes precedence.

Parameter	Type	Description
member_type	String	Specifies the type of the backend server. Value options: • **ip**: IP as backend servers • **instance**: ECSs used as backend servers
instance_id	String	Specifies the ID of the instance associated with the backend server. If this parameter is left blank, the backend server is not an ECS. It may be an IP address.
port_id	String	Specifies the ID of the VPC port bound to the IP address.
ret_status	String	Specifies the status of adding a backend server. Value options: • **successful**: The backend server is added. • **existed**: The backend server already exists.
created_at	String	Specifies the time when the backend servers were added. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
updated_at	String	Specifies the time when the backend servers were updated. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.

Table 5-455 MemberStatus

Parameter	Type	Description
listener_id	String	Specifies the listener ID.
operating_status	String	Specifies the health status of the backend server. Value options: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group to which the backend server belongs. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist.
reason	**MemberHealthCheckFailedReason** object	Specifies why health check fails.

Table 5-456 MemberHealthCheckFailedReason

Parameter	Type	Description
reason_code	String	Specifies the code of the health check failures. Value options: • **CONNECT_TIMEOUT**: The connection with the backend server times out during a health check. • **CONNECT_REFUSED**: The load balancer rejects connections with the backend server during a health check. • **CONNECT_FAILED**: The load balancer fails to establish connections with the backend server during a health check. • **CONNECT_INTERRUPT**: The load balancer is disconnected from the backend server during a health check. • **SSL_HANDSHAKE_ERROR**: The SSL handshakes with the backend server fail during a health check. • **RECV_RESPONSE_FAILED**: The load balancer fails to receive responses from the backend server during a health check. • **RECV_RESPONSE_TIMEOUT**: The load balancer does not receive responses from the backend server within the timeout duration during a health check. • **SEND_REQUEST_FAILED**: The load balancer fails to send a health check request to the backend server during a health check. • **SEND_REQUEST_TIMEOUT**: The load balancer fails to send a health check request to the backend server within the timeout duration. • **RESPONSE_FORMAT_ERROR**: The load balancer receives invalid responses from the backend server during a health check. • **RESPONSE_MISMATCH**: The response code received from the

Parameter	Type	Description
		backend server is different from the preset code.
expected_response	String	Specifies the expected HTTP status code. This parameter will take effect only when **type** is set to **HTTP**, **HTTPS**, or **GRPC**. The status code cannot be **null** if **reason_code** is **RESPONSE_MISMATCH**. Value ranges: ● A specific status code. If **type** is set to **GRPC**, the status code ranges from 0 to 99. If **type** is set to other values, the status code ranges from 200 to 599. For example, the status code can be **0** or **200**. ● A list of status codes that are separated with commas (,), for example, **200,202** or **0,1**. A maximum of five status codes are supported. ● A status code range. Different ranges are separated with commas (,), for example, **200-204,300-399** or **0-5,10-12,20-30**. A maximum of five ranges are supported.
healthcheck_response	String	Specifies the returned HTTP status code in the response. This parameter will take effect only when **type** is set to **HTTP**, **HTTPS**, or **GRPC**. The status code cannot be **null** if **reason_code** is **RESPONSE_MISMATCH**. Value range: A specific status code. If **type** is set to **GRPC**, the status code ranges from 0 to 99. If **type** is set to other values, the status code ranges from 200 to 599. For example, the status code can be **0** or **200**.

Example Requests

Batch adding backend servers


```
POST https://{ELB_Endpoint}/v3/04dd36f964000fe22f9ac00bc85b1a1d/elb/pools/04a9bc65-b75b-478d-b4d6-e693bb61dd35/members/batch-add

{
  "members" : [ {
    "name" : "lzs_batch_member1",
    "weight" : 1,
    "address" : "192.168.0.48",
    "protocol_port" : 8080,
    "subnet_cidr_id" : "61da8098-954b-4809-bc5a-b99ccef8a398"
  }, {
    "name" : "lzs_batch_member2",
    "weight" : 1,
    "address" : "192.168.0.49",
    "protocol_port" : 8080,
    "subnet_cidr_id" : "61da8098-954b-4809-bc5a-b99ccef8a398"
  } ]
}
```

Example Responses

Status code: 201

Normal response to POST requests.

```
{
  "request_id" : "b5d8bb34d28f3e47b352c14419e8fe04",
  "members" : [ {
    "weight" : 1,
    "admin_state_up" : false,
    "project_id" : "04dd36f964000fe22f9ac00bc85b1a1d",
    "address" : "192.168.0.48",
    "protocol_port" : 8080,
    "id" : "9346ad28-6971-456a-9711-2917d023930a",
    "operating_status" : "OFFLINE",
    "instance_id" : "",
    "member_type" : "instance",
    "port_id" : "",
    "name" : "batch_member1",
    "subnet_cidr_id" : "61da8098-954b-4809-bc5a-b99ccef8a398",
    "ret_status" : "successful"
  }, {
    "weight" : 1,
    "admin_state_up" : false,
    "project_id" : "04dd36f964000fe22f9ac00bc85b1a1d",
    "address" : "192.168.0.49",
    "protocol_port" : 8080,
    "id" : "94548801-1023-452f-bcf7-6174e77cb772",
    "operating_status" : "OFFLINE",
    "instance_id" : "",
    "member_type" : "instance",
    "port_id" : "",
    "name" : "batch_member2",
    "subnet_cidr_id" : "61da8098-954b-4809-bc5a-b99ccef8a398",
    "ret_status" : "successful"
  } ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Batch adding backend servers


```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;

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

public class BatchCreateMembersSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        BatchCreateMembersRequest request = new BatchCreateMembersRequest();
        request.withPoolId("{pool_id}");
        BatchCreateMembersRequestBody body = new BatchCreateMembersRequestBody();
        List<BatchCreateMembersOption> listbodyMembers = new ArrayList<>();
        listbodyMembers.add(
            new BatchCreateMembersOption()
                .withName("lzs_batch_member1")
                .withAddress("192.168.0.48")
                .withProtocolPort(8080)
                .withSubnetCidrId("61da8098-954b-4809-bc5a-b99ccef8a398")
                .withWeight(1)
        );
        listbodyMembers.add(
            new BatchCreateMembersOption()
                .withName("lzs_batch_member2")
                .withAddress("192.168.0.49")
                .withProtocolPort(8080)
                .withSubnetCidrId("61da8098-954b-4809-bc5a-b99ccef8a398")
                .withWeight(1)
        );
        body.withMembers(listbodyMembers);
        request.withBody(body);
        try {
            BatchCreateMembersResponse response = client.batchCreateMembers(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

Batch adding backend servers

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = BatchCreateMembersRequest()
        request.pool_id = "{pool_id}"
        listMembersbody = [
            BatchCreateMembersOption(
                name="lzs_batch_member1",
                address="192.168.0.48",
                protocol_port=8080,
                subnet_cidr_id="61da8098-954b-4809-bc5a-b99ccef8a398",
                weight=1
            ),
            BatchCreateMembersOption(
                name="lzs_batch_member2",
                address="192.168.0.49",
                protocol_port=8080,
                subnet_cidr_id="61da8098-954b-4809-bc5a-b99ccef8a398",
                weight=1
            )
        ]
        request.body = BatchCreateMembersRequestBody(
            members=listMembersbody
        )
        response = client.batch_create_members(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

Batch adding backend servers


```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.BatchCreateMembersRequest{}
    request.PoolId = "{pool_id}"
    nameMembers:= "lzs_batch_member1"
    subnetCidrIdMembers:= "61da8098-954b-4809-bc5a-b99ccef8a398"
    weightMembers:= int32(1)
    nameMembers1:= "lzs_batch_member2"
    subnetCidrIdMembers1:= "61da8098-954b-4809-bc5a-b99ccef8a398"
    weightMembers1:= int32(1)
    var listMembersbody = []model.BatchCreateMembersOption{
        {
            Name: &nameMembers,
            Address: "192.168.0.48",
            ProtocolPort: int32(8080),
            SubnetCidrId: &subnetCidrIdMembers,
            Weight: &weightMembers,
        },
        {
            Name: &nameMembers1,
            Address: "192.168.0.49",
            ProtocolPort: int32(8080),
            SubnetCidrId: &subnetCidrIdMembers1,
            Weight: &weightMembers1,
        },
    }
    request.Body = &model.BatchCreateMembersRequestBody{
        Members: listMembersbody,
    }
    response, err := client.BatchCreateMembers(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 POST requests.

Error Codes

See **Error Codes**.

5.12.8 Batch Deleting Backend Servers

Function

This API is used to delete backend servers from the specified backend server group in batches. You can remove up to 200 backend servers at a time from a backend server group.

Calling Method

For details, see **Calling APIs**.

URI

POST /v3/{project_id}/elb/pools/{pool_id}/members/batch-delete

Table 5-457 Path Parameters

Parameter	Mandatory	Type	Description
pool_id	Yes	String	Specifies the ID of the backend server group.
project_id	Yes	String	Specifies the project ID.

Request Parameters

Table 5-458 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Table 5-459 Request body parameters

Parameter	Mandatory	Type	Description
members	Yes	Array of **BatchDeleteMembersOption** objects	Specifies the request body for deleting backend servers in batches.

Table 5-460 BatchDeleteMembersOption

Parameter	Mandatory	Type	Description
id	No	String	Specifies the ID of the backend server to be deleted. Note: If **id** is passed, other parameters cannot be specified. Otherwise, an error will be reported. The value of this parameter is not the ID of the server but an ID automatically generated for the backend server that has already been associated with the load balancer.
address	No	String	Specifies the IP address bound to the backend server. Note: • **address** and **protocol_port** must be passed at the same time. • **id** cannot be passed together with **address** and **protocol_port**.

Parameter	Mandatory	Type	Description
protocol_port	No	Integer	Specifies the port used by the backend server to receive requests. Note: • **address** and **protocol_port** must be passed at the same time. • **id** cannot be passed together with **address** and **protocol_port**. • This parameter can be set to **0**, which is used to remove a backend server from its backend server group whose **Forward to Same Port** is enabled.

Response Parameters

Status code: 200

Table 5-461 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
members	Array of **BatchDeleteMembersState** objects	Specifies the backend servers.

Table 5-462 BatchDeleteMembersState

Parameter	Type	Description
id	String	Specifies the backend server ID. Note: The value of this parameter is not the ID of the server but an ID automatically generated for the backend server that has already been associated with the load balancer.

Parameter	Type	Description
ret_status	String	Specifies the status of deleting the backend server. Value options: • **successful**: The backend server is deleted. • **not found**: The backend server does not exist.

Example Requests

- Deleting backend servers in batches by IDs

```
POST https://{ELB_Endpoint}/v3/04dd36f964000fe22f9ac00bc85b1a1d/elb/pools/04a9bc65-b75b-478d-b4d6-e693bb61dd35/members/batch-delete

{
  "members" : [ {
    "id" : "141a8dea-b3f9-4fed-a1e2-30678f53de0b"
  }, {
    "id" : "14d0a82b-fcc2-4ce8-aac8-96d86a7973e4"
  } ]
}
```

- Deleting backend servers in batches by IP addresses and ports

```
POST https://{ELB_Endpoint}/v3/04dd36f964000fe22f9ac00bc85b1a1d/elb/pools/04a9bc65-b75b-478d-b4d6-e693bb61dd35/members/batch-delete

{
  "members" : [ {
    "address" : "192.168.0.48",
    "protocol_port" : 8080
  }, {
    "address" : "192.168.0.49",
    "protocol_port" : 8080
  } ]
}
```

Example Responses

Status code: 200

Normal response to POST requests.

```
{
  "request_id" : "db97a1d3c5ee386729dc00e4df1d5708",
  "members" : [ {
    "id" : "141a8dea-b3f9-4fed-a1e2-30678f53de0b",
    "ret_status" : "not found"
  }, {
    "id" : "14d0a82b-fcc2-4ce8-aac8-96d86a7973e4",
    "ret_status" : "successful"
  } ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

- Deleting backend servers in batches by IDs

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;

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

public class BatchDeleteMembersSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        BatchDeleteMembersRequest request = new BatchDeleteMembersRequest();
        request.withPoolId("{pool_id}");
        BatchDeleteMembersRequestBody body = new BatchDeleteMembersRequestBody();
        List<BatchDeleteMembersOption> listbodyMembers = new ArrayList<>();
        listbodyMembers.add(
            new BatchDeleteMembersOption()
                .withId("141a8dea-b3f9-4fed-a1e2-30678f53de0b")
        );
        listbodyMembers.add(
            new BatchDeleteMembersOption()
                .withId("14d0a82b-fcc2-4ce8-aac8-96d86a7973e4")
        );
        body.withMembers(listbodyMembers);
        request.withBody(body);
        try {
            BatchDeleteMembersResponse response = client.batchDeleteMembers(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());
        }
    }
}
```


- Deleting backend servers in batches by IP addresses and ports

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;

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

public class BatchDeleteMembersSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        BatchDeleteMembersRequest request = new BatchDeleteMembersRequest();
        request.withPoolId("{pool_id}");
        BatchDeleteMembersRequestBody body = new BatchDeleteMembersRequestBody();
        List<BatchDeleteMembersOption> listbodyMembers = new ArrayList<>();
        listbodyMembers.add(
            new BatchDeleteMembersOption()
                .withAddress("192.168.0.48")
                .withProtocolPort(8080)
        );
        listbodyMembers.add(
            new BatchDeleteMembersOption()
                .withAddress("192.168.0.49")
                .withProtocolPort(8080)
        );
        body.withMembers(listbodyMembers);
        request.withBody(body);
        try {
            BatchDeleteMembersResponse response = client.batchDeleteMembers(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

- Deleting backend servers in batches by IDs

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = BatchDeleteMembersRequest()
        request.pool_id = "{pool_id}"
        listMembersbody = [
            BatchDeleteMembersOption(
                id="141a8dea-b3f9-4fed-a1e2-30678f53de0b"
            ),
            BatchDeleteMembersOption(
                id="14d0a82b-fcc2-4ce8-aac8-96d86a7973e4"
            )
        ]
        request.body = BatchDeleteMembersRequestBody(
            members=listMembersbody
        )
        response = client.batch_delete_members(request)
        print(response)
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)
```

- Deleting backend servers in batches by IP addresses and ports

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = BatchDeleteMembersRequest()
        request.pool_id = "{pool_id}"
        listMembersbody = [
            BatchDeleteMembersOption(
                address="192.168.0.48",
                protocol_port=8080
            ),
            BatchDeleteMembersOption(
                address="192.168.0.49",
                protocol_port=8080
            )
        ]
        request.body = BatchDeleteMembersRequestBody(
            members=listMembersbody
        )
        response = client.batch_delete_members(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

- Deleting backend servers in batches by IDs

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())
```



```
    request := &model.BatchDeleteMembersRequest{}
    request.PoolId = "{pool_id}"
    idMembers:= "141a8dea-b3f9-4fed-a1e2-30678f53de0b"
    idMembers1:= "14d0a82b-fcc2-4ce8-aac8-96d86a7973e4"
    var listMembersbody = []model.BatchDeleteMembersOption{
        {
            Id: &idMembers,
        },
        {
            Id: &idMembers1,
        },
    }
    request.Body = &model.BatchDeleteMembersRequestBody{
        Members: listMembersbody,
    }
    response, err := client.BatchDeleteMembers(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

- Deleting backend servers in batches by IP addresses and ports

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.BatchDeleteMembersRequest{}
    request.PoolId = "{pool_id}"
    addressMembers:= "192.168.0.48"
    protocolPortMembers:= int32(8080)
    addressMembers1:= "192.168.0.49"
    protocolPortMembers1:= int32(8080)
    var listMembersbody = []model.BatchDeleteMembersOption{
        {
            Address: &addressMembers,
            ProtocolPort: &protocolPortMembers,
        },
        {
            Address: &addressMembers1,
```



```
            ProtocolPort: &protocolPortMembers1,
        },
    }
    request.Body = &model.BatchDeleteMembersRequestBody{
        Members: listMembersbody,
    }
    response, err := client.BatchDeleteMembers(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 POST requests.

Error Codes

See **Error Codes**.

5.12.9 Batch Updating Backend Servers

Function

This API is used to update backend servers in a given backend server group in batches. You can update up to 200 backend servers at a time from a backend server group.

Calling Method

For details, see **Calling APIs**.

URI

POST /v3/{project_id}/elb/pools/{pool_id}/members/batch-update

Table 5-463 Path Parameters

Parameter	Mandatory	Type	Description
pool_id	Yes	String	Specifies the ID of the backend server group.
project_id	Yes	String	Specifies the project ID.

Request Parameters

Table 5-464 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Table 5-465 Request body parameters

Parameter	Mandatory	Type	Description
members	Yes	Array of **BatchUpdateMembersOption** objects	Specifies the backend server.

Table 5-466 BatchUpdateMembersOption

Parameter	Mandatory	Type	Description
id	Yes	String	Specifies the backend server ID. Note: The value of this parameter is not the ID of the server but an ID automatically generated for the backend server that has already been associated with the load balancer.
admin_state_up	No	Boolean	Specifies the administrative status of the backend server. The value can be **true** or **false**. Although this parameter can be used in the APIs for creating and updating backend servers, its actual value depends on whether ECSs exist. If ECSs exist, the value is **true**. Otherwise, the value is **false**. Please do not specify this parameter.

Parameter	Mandatory	Type	Description
name	No	String	Specifies the backend server name.
protocol_port	No	Integer	Specifies the port used by the backend server to receive requests. **NOTE** This parameter cannot be updated if **any_port_enable** is set to **true** for a backend server group.
weight	No	Integer	Specifies the weight of the backend server. Requests are routed to backend servers in the backend server group based on their weights. If the weight is set to **0**, the backend server will not accept new requests. This parameter is invalid when **lb_algorithm** of the backend server group to which the backend server belongs is set to **SOURCE_IP**.

Response Parameters

Status code: 200

Table 5-467 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
members	Array of **BatchUpdateMember** objects	Specifies the backend servers.

Table 5-468 BatchUpdateMember

Parameter	Type	Description
id	String	Specifies the backend server ID. Note: The value of this parameter is not the ID of the server but an ID automatically generated for the backend server that has already been associated with the load balancer.
name	String	Specifies the backend server name.
project_id	String	Specifies the ID of the project where the backend server is used.
admin_state_up	Boolean	Specifies the administrative status of the backend server. The value can be **true** or **false**. Although this parameter can be used in the APIs for creating and updating backend servers, its actual value depends on whether ECSs exist. If ECSs exist, the value is **true**. Otherwise, the value is **false**.

Parameter	Type	Description
subnet_cidr_id	String	Specifies the ID of the IPv4 or IPv6 subnet where the backend server resides. **neutron_subnet_id** defines IPv4 subnets, and **neutron_network_id** defines IPv6 subnets. You can query parameters **neutron_subnet_id** and **neutron_network_id** in the response by calling the API GET https://{VPC_Endpoint}/v1/{project_id}/subnets to get the IPv4 subnet ID and IPv6 subnet ID respectively. Note: • The IPv4 or IPv6 subnet must be in the same VPC as the subnet of the load balancer. • If **ip_target_enable** is set to **true**, this parameter can be left blank. In this case, IP as backend servers must use private IPv4 addresses, and the protocol of the backend server group must be TCP, UDP, TLS, HTTP, HTTPS, QUIC, or GRPC. • If **ip_target_enable** is set to **false**, this parameter must be specified.
protocol_port	Integer	Specifies the port used by the backend server to receive requests. Note: • This parameter can be left blank because it does not take effect if **any_port_enable** is set to **true** for a backend server group.
weight	Integer	Specifies the weight of the backend server. Requests are routed to backend servers in the same backend server group based on their weights. The value ranges from **0** to **100**, and the default value is **1**. The larger the weight is, the higher proportion of requests the backend server receives. If the weight is set to 0, the backend server will not accept new requests. If **lb_algorithm** is set to **SOURCE_IP** or **QUIC_CID**, this parameter will not take effect.

Parameter	Type	Description
address	String	Specifies the private IP address bound to the backend server. Note: • If **subnet_cidr_id** is left blank, **IP as a Backend** is enabled. In this case, the IP address must be an IPv4 address. • If **subnet_cidr_id** is not left blank, the IP address can be IPv4 or IPv6. It must be in the subnet specified by **subnet_cidr_id**.
operating_status	String	Specifies the operating status of the backend server. Value options: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group to which the backend server belongs. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist.
reason	**MemberHealthCheckFailedReason** object	Specifies why health check fails.
status	Array of **MemberStatus** objects	Specifies the health status of the backend server if **listener_id** under **status** is specified. If **listener_id** under **status** is not specified, **operating_status** of **member** takes precedence.
member_type	String	Specifies the type of the backend server. Value options: • **ip**: IP addresses added as backend servers • **instance**: ECSs used as backend servers
instance_id	String	Specifies the ID of the instance associated with the backend server. If this parameter is left blank, the backend server is not an ECS. It may be an IP address.

Parameter	Type	Description
port_id	String	Specifies the ID of the VPC port bound to the IP address.
created_at	String	Specifies the time when the backend servers were added. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
updated_at	String	Specifies the time when the backend servers were updated. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.

Table 5-469 MemberStatus

Parameter	Type	Description
listener_id	String	Specifies the listener ID.
operating_status	String	Specifies the health status of the backend server. Value options: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group to which the backend server belongs. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist.
reason	**MemberHealthCheckFailedReason** object	Specifies why health check fails.

Table 5-470 MemberHealthCheckFailedReason

Parameter	Type	Description
reason_code	String	Specifies the code of the health check failures. Value options: • **CONNECT_TIMEOUT**: The connection with the backend server times out during a health check. • **CONNECT_REFUSED**: The load balancer rejects connections with the backend server during a health check. • **CONNECT_FAILED**: The load balancer fails to establish connections with the backend server during a health check. • **CONNECT_INTERRUPT**: The load balancer is disconnected from the backend server during a health check. • **SSL_HANDSHAKE_ERROR**: The SSL handshakes with the backend server fail during a health check. • **RECV_RESPONSE_FAILED**: The load balancer fails to receive responses from the backend server during a health check. • **RECV_RESPONSE_TIMEOUT**: The load balancer does not receive responses from the backend server within the timeout duration during a health check. • **SEND_REQUEST_FAILED**: The load balancer fails to send a health check request to the backend server during a health check. • **SEND_REQUEST_TIMEOUT**: The load balancer fails to send a health check request to the backend server within the timeout duration. • **RESPONSE_FORMAT_ERROR**: The load balancer receives invalid responses from the backend server during a health check. • **RESPONSE_MISMATCH**: The response code received from the

Parameter	Type	Description
		backend server is different from the preset code.
expected_response	String	Specifies the expected HTTP status code. This parameter will take effect only when **type** is set to **HTTP**, **HTTPS**, or **GRPC**. The status code cannot be **null** if **reason_code** is **RESPONSE_MISMATCH**. Value ranges: ● A specific status code. If **type** is set to **GRPC**, the status code ranges from 0 to 99. If **type** is set to other values, the status code ranges from 200 to 599. For example, the status code can be **0** or **200**. ● A list of status codes that are separated with commas (,), for example, **200,202** or **0,1**. A maximum of five status codes are supported. ● A status code range. Different ranges are separated with commas (,), for example, **200-204,300-399** or **0-5,10-12,20-30**. A maximum of five ranges are supported.
healthcheck_response	String	Specifies the returned HTTP status code in the response. This parameter will take effect only when **type** is set to **HTTP**, **HTTPS**, or **GRPC**. The status code cannot be **null** if **reason_code** is **RESPONSE_MISMATCH**. Value range: A specific status code. If **type** is set to **GRPC**, the status code ranges from 0 to 99. If **type** is set to other values, the status code ranges from 200 to 599. For example, the status code can be **0** or **200**.

Example Requests

Modifying backend servers in batches


```
POST https://{ELB_Endpoint}/v3/04dd36f964000fe22f9ac00bc85b1a1d/elb/pools/04a9bc65-b75b-478d-b4d6-e693bb61dd35/members/batch-update

{
  "members" : [ {
    "name" : "batch_update_member1",
    "weight" : 1,
    "admin_state_up" : true,
    "protocol_port" : 8080,
    "id" : "61da8098-954b-4809-bc5a-b99ccef8a398"
  }, {
    "name" : "batch_update_member2",
    "weight" : 2,
    "admin_state_up" : true,
    "protocol_port" : 8081,
    "id" : "61da8098-954b-4809-bc5a-b99ccef8a398"
  } ]
}
```

Example Responses

Status code: 200

Successful request.

```
{
  "request_id" : "b5d8bb34d28f3e47b352c14419e8fe04",
  "members" : [ {
    "weight" : 1,
    "admin_state_up" : false,
    "project_id" : "04dd36f964000fe22f9ac00bc85b1a1d",
    "address" : "192.168.0.48",
    "protocol_port" : 8080,
    "id" : "9346ad28-6971-456a-9711-2917d023930a",
    "operating_status" : "OFFLINE",
    "name" : "batch_member1",
    "subnet_cidr_id" : "61da8098-954b-4809-bc5a-b99ccef8a398"
  }, {
    "weight" : 1,
    "admin_state_up" : false,
    "project_id" : "04dd36f964000fe22f9ac00bc85b1a1d",
    "address" : "192.168.0.49",
    "protocol_port" : 8080,
    "id" : "94548801-1023-452f-bcf7-6174e77cb772",
    "operating_status" : "OFFLINE",
    "name" : "batch_member2",
    "subnet_cidr_id" : "61da8098-954b-4809-bc5a-b99ccef8a398"
  } ]
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Modifying backend servers in batches

```
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.elb.v3.region.ElbRegion;
```



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

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

public class BatchUpdateMembersSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        BatchUpdateMembersRequest request = new BatchUpdateMembersRequest();
        request.withPoolId("{pool_id}");
        BatchUpdateMembersRequestBody body = new BatchUpdateMembersRequestBody();
        List<BatchUpdateMembersOption> listbodyMembers = new ArrayList<>();
        listbodyMembers.add(
            new BatchUpdateMembersOption()
                .withId("61da8098-954b-4809-bc5a-b99ccef8a398")
                .withAdminStateUp(true)
                .withName("batch_update_member1")
                .withProtocolPort(8080)
                .withWeight(1)
        );
        listbodyMembers.add(
            new BatchUpdateMembersOption()
                .withId("61da8098-954b-4809-bc5a-b99ccef8a398")
                .withAdminStateUp(true)
                .withName("batch_update_member2")
                .withProtocolPort(8081)
                .withWeight(2)
        );
        body.withMembers(listbodyMembers);
        request.withBody(body);
        try {
            BatchUpdateMembersResponse response = client.batchUpdateMembers(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

Modifying backend servers in batches

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = BatchUpdateMembersRequest()
        request.pool_id = "{pool_id}"
        listMembersbody = [
            BatchUpdateMembersOption(
                id="61da8098-954b-4809-bc5a-b99ccef8a398",
                admin_state_up=True,
                name="batch_update_member1",
                protocol_port=8080,
                weight=1
            ),
            BatchUpdateMembersOption(
                id="61da8098-954b-4809-bc5a-b99ccef8a398",
                admin_state_up=True,
                name="batch_update_member2",
                protocol_port=8081,
                weight=2
            )
        ]
        request.body = BatchUpdateMembersRequestBody(
            members=listMembersbody
        )
        response = client.batch_update_members(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

Modifying backend servers in batches

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.BatchUpdateMembersRequest{}
    request.PoolId = "{pool_id}"
    adminStateUpMembers:= true
    nameMembers:= "batch_update_member1"
    protocolPortMembers:= int32(8080)
    weightMembers:= int32(1)
    adminStateUpMembers1:= true
    nameMembers1:= "batch_update_member2"
    protocolPortMembers1:= int32(8081)
    weightMembers1:= int32(2)
    var listMembersbody = []model.BatchUpdateMembersOption{
        {
            Id: "61da8098-954b-4809-bc5a-b99ccef8a398",
            AdminStateUp: &adminStateUpMembers,
            Name: &nameMembers,
            ProtocolPort: &protocolPortMembers,
            Weight: &weightMembers,
        },
        {
            Id: "61da8098-954b-4809-bc5a-b99ccef8a398",
            AdminStateUp: &adminStateUpMembers1,
            Name: &nameMembers1,
            ProtocolPort: &protocolPortMembers1,
            Weight: &weightMembers1,
        },
    }
    request.Body = &model.BatchUpdateMembersRequestBody{
        Members: listMembersbody,
    }
    response, err := client.BatchUpdateMembers(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	Successful request.

Error Codes

See **Error Codes**.

5.13 Health Check

5.13.1 Configuring a Health Check

Function

This API is used to configure a health check.

Constraints

The security groups must have rules that allow traffic to 100.125.0.0/16.

If you want to use UDP for health checks, ensure that the protocol of the backend server group is UDP.

Calling Method

For details, see **Calling APIs**.

URI

POST /v3/{project_id}/elb/healthmonitors

Table 5-471 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Request Parameters

Table 5-472 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Table 5-473 Request body parameters

Parameter	Mandatory	Type	Description
healthmonitor	Yes	**CreateHealthMonitorOption** object	Specifies the health check.

Table 5-474 CreateHealthMonitorOption

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Specifies the administrative status of the health check. • **true** (default): Health check is enabled. • **false**: Health check is disabled.
delay	Yes	Integer	Specifies the interval between health checks, in seconds. The value ranges from **1** to **50**.
domain_name	No	String	Specifies the domain name that HTTP requests are sent to during the health check. The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter. The value is left blank by default, indicating that the virtual IP address of the load balancer is used as the destination address of HTTP requests. This parameter is available only when **type** is set to **HTTP** or **HTTPS**.

Parameter	Mandatory	Type	Description
expected_codes	No	String	Specifies the expected HTTP status code. Value options: • A specific value, for example, 200 • A list of values that are separated with commas (,), for example, 200, 202 • A value range, for example, 200-204 If **type** is set to **GRPC**, the default value is **0**. If **type** is set to other protocols, the default value is **200**. This parameter will take effect only when **type** is set to **HTTP**, **HTTPS** or **GRPC**.
http_method	No	String	Specifies the HTTP method. The value can be **GET**, **HEAD**, or **POST**. The default value is **GET**. This parameter is available when **type** is set to **HTTP** or **HTTPS**.
max_retries	Yes	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **OFFLINE** to **ONLINE**. The value ranges from **1** to **10**.
max_retries_down	No	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **ONLINE** to **OFFLINE**. The value ranges from **1** to **10**, and the default value is **3**.

Parameter	Mandatory	Type	Description
monitor_port	No	Integer	Specifies the port used for the health check. Note: • This parameter is required if **any_port_enable** is set to **true** for the backend server group. Value range: **1** to **65535**, or **null** (the port of a backend server will be used by default) Default value: **null**
name	No	String	Specifies the health check name.
pool_id	Yes	String	Specifies the ID of the backend server group for which the health check is configured.
project_id	No	String	Specifies the project ID.
timeout	Yes	Integer	Specifies the maximum time required for waiting for a response from the health check, in seconds. It is recommended that you set the value less than that of parameter **delay**.

Parameter	Mandatory	Type	Description
type	Yes	String	Specifies the health check protocol. The value can be **TCP**, **UDP_CONNECT**, **HTTP**, **HTTPS**, **GRPC**, or **TLS**. Note: • If the protocol of the backend server is QUIC, the value can only be **UDP_CONNECT**. • If the protocol of the backend server is UDP, the value can only be **UDP_CONNECT**. • If the protocol of the backend server is TCP, the value can only be **TCP**, **HTTP**, or **HTTPS**. • If the protocol of the backend server is HTTP, the value can only be **TCP**, **HTTP**, **HTTPS**, **GRPC**, or **TLS**. • If the protocol of the backend server is HTTPS, the value can only be **TCP**, **HTTP**, **HTTPS**, **GRPC**, or **TLS**. • If the protocol of the backend server is GRPC, the value can only be **TCP**, **HTTP**, **HTTPS**, **GRPC**, or **TLS**. • If the protocol of the backend server is TLS, the value can only be **TCP**, **HTTP**, **HTTPS**, **GRPC**, or **TLS**.

Parameter	Mandatory	Type	Description
url_path	No	String	Specifies the HTTP request path for the health check. The value must start with a slash (/), and the default value is **/**. The value can contain letters, digits, hyphens (-), slashes (/), periods (.), percentage signs (%), question marks (?), pound signs (#), ampersand signs (&), and the extended character set: _;~!()*[]@$^:',+. Note: This parameter is available only when **type** is set to **HTTP** or **HTTPS**.

Response Parameters

Status code: 201

Table 5-475 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
healthmonitor	**HealthMonitor** object	Specifies the health check.

Table 5-476 HealthMonitor

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the health check. • **true** (default) indicates that the health check is enabled. • **false** indicates that the health check is disabled.
delay	Integer	Specifies the interval between health checks, in seconds. The value ranges from **1** to **50**.

Parameter	Type	Description
domain_name	String	Specifies the domain name that HTTP requests are sent to during the health check. The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter. The value is left blank by default, indicating that the virtual IP address of the load balancer is used as the destination address of HTTP requests. This parameter is available only when **type** is set to **HTTP** or **HTTPS**.
expected_codes	String	Specifies the expected HTTP status code. Value options: ● A specific value, for example, 200 ● A list of values that are separated with commas (,), for example, 200, 202 ● A value range, for example, 200-204 If **type** is set to **GRPC**, the default value is **0**. If **type** is set to other protocols, the default value is **200**. This parameter will take effect only when **type** is set to **HTTP**, **HTTPS** or **GRPC**.
http_method	String	Specifies the HTTP method. The value can be **GET**, **HEAD**, or **POST**. The default value is **GET**. This parameter is available when **type** is set to **HTTP** or **HTTPS**.
id	String	Specifies the health check ID.
max_retries	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **OFFLINE** to **ONLINE**. The value ranges from **1** to **10**.

Parameter	Type	Description
max_retries_down	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **ONLINE** to **OFFLINE**. The value ranges from **1** to **10**, and the default value is **3**.
monitor_port	Integer	Specifies the port used for the health check. Value range: **1** to **65535**, or **null** (the port of a backend server will be used by default) Default value: **null**
name	String	Specifies the health check name.
pools	Array of **PoolRef** objects	Lists the IDs of backend server groups for which the health check is configured. Only one ID will be returned.
project_id	String	Specifies the project ID.
timeout	Integer	Specifies the maximum time required for waiting for a response from the health check, in seconds. It is recommended that you set the value less than that of parameter **delay**.

Parameter	Type	Description
type	String	Specifies the health check protocol. The value can be **TCP**, **UDP_CONNECT**, **HTTP**, **HTTPS**, **GRPC**, or **TLS**. Note: • If the protocol of the backend server is QUIC, the value can only be **UDP_CONNECT**. • If the protocol of the backend server is UDP, the value can only be **UDP_CONNECT**. • If the protocol of the backend server is TCP, the value can only be **TCP**, **HTTP**, or **HTTPS**. • If the protocol of the backend server is HTTP, the value can only be **TCP**, **HTTP**, **HTTPS**, **GRPC**, or **TLS**. • If the protocol of the backend server is HTTPS, the value can only be **TCP**, **HTTP**, **HTTPS**, **GRPC**, or **TLS**. • If the protocol of the backend server is GRPC, the value can only be **TCP**, **HTTP**, **HTTPS**, **GRPC**, or **TLS**. • If the protocol of the backend server is TLS, the value can only be **TCP**, **HTTP**, **HTTPS**, **GRPC**, or **TLS**.
url_path	String	Specifies the HTTP request path for the health check. The value must start with a slash (/), and the default value is **/**. The value can contain letters, digits, hyphens (-), slashes (/), periods (.), percentage signs (%), question marks (?), pound signs (#), ampersand signs (&), and the extended character set: _;~!()*[]@$^:',+. Note: This parameter is available only when **type** is set to **HTTP** or **HTTPS**.

Parameter	Type	Description
created_at	String	Specifies the time when the health check was configured. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
updated_at	String	Specifies the time when the health check was updated. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.

Table 5-477 PoolRef

Parameter	Type	Description
id	String	Specifies the ID of the backend server group.

Example Requests

Configuring a health check for an HTTP backend server group

```
POST https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/healthmonitors

{
  "healthmonitor" : {
    "name" : "My Healthmonitor",
    "max_retries" : 3,
    "pool_id" : "488acc50-6bcf-423d-8f0a-0f4184f5b8a0",
    "type" : "HTTP",
    "timeout" : 30,
    "delay" : 1
  }
}
```

Example Responses

Status code: 201

Normal response to POST requests.


```
{
  "request_id" : "0e837340-f1bd-4037-8f61-9923d0f0b19e",
  "healthmonitor" : {
    "monitor_port" : null,
    "id" : "c2b210b2-60c4-449d-91e2-9e9ea1dd7441",
    "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
    "domain_name" : null,
    "name" : "My Healthmonitor",
    "delay" : 1,
    "max_retries" : 3,
    "pools" : [ {
      "id" : "488acc50-6bcf-423d-8f0a-0f4184f5b8a0"
    } ],
    "admin_state_up" : true,
    "timeout" : 30,
    "type" : "HTTP",
    "expected_codes" : "200",
    "url_path" : "/",
    "http_method" : "GET"
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Configuring a health check for an HTTP backend server group

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class CreateHealthMonitorSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateHealthMonitorRequest request = new CreateHealthMonitorRequest();
        CreateHealthMonitorRequestBody body = new CreateHealthMonitorRequestBody();
        CreateHealthMonitorOption healthmonitorbody = new CreateHealthMonitorOption();
        healthmonitorbody.withDelay(1)
```



```
            .withMaxRetries(3)
            .withName("My Healthmonitor")
            .withPoolId("488acc50-6bcf-423d-8f0a-0f4184f5b8a0")
            .withTimeout(30)
            .withType("HTTP");
        body.withHealthmonitor(healthmonitorbody);
        request.withBody(body);
        try {
            CreateHealthMonitorResponse response = client.createHealthMonitor(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

Configuring a health check for an HTTP backend server group

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateHealthMonitorRequest()
        healthmonitorbody = CreateHealthMonitorOption(
            delay=1,
            max_retries=3,
            name="My Healthmonitor",
            pool_id="488acc50-6bcf-423d-8f0a-0f4184f5b8a0",
            timeout=30,
            type="HTTP"
        )
        request.body = CreateHealthMonitorRequestBody(
            healthmonitor=healthmonitorbody
        )
        response = client.create_health_monitor(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

Configuring a health check for an HTTP backend server group

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateHealthMonitorRequest{}
    nameHealthmonitor:= "My Healthmonitor"
    healthmonitorbody := &model.CreateHealthMonitorOption{
        Delay: int32(1),
        MaxRetries: int32(3),
        Name: &nameHealthmonitor,
        PoolId: "488acc50-6bcf-423d-8f0a-0f4184f5b8a0",
        Timeout: int32(30),
        Type: "HTTP",
    }
    request.Body = &model.CreateHealthMonitorRequestBody{
        Healthmonitor: healthmonitorbody,
    }
    response, err := client.CreateHealthMonitor(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 POST requests.

Error Codes

See **Error Codes**.

5.13.2 Querying Health Checks

Function

This API is used to query all health checks.

Constraints

This API has the following constraints:

- Parameters **marker**, **limit**, and **page_reverse** are used for pagination query.
- Parameters **marker** and **page_reverse** take effect only when they are used together with parameter **limit**.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/healthmonitors

Table 5-478 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Table 5-479 Query Parameters

Parameter	Mandatory	Type	Description
marker	No	String	Specifies the ID of the last record on the previous page. Note: • This parameter must be used together with **limit**. • If this parameter is not specified, the first page will be queried. • This parameter cannot be left blank or set to an invalid ID.
limit	No	Integer	Specifies the number of records on each page. Value range: 0–2000 Default value: 2000
page_reverse	No	Boolean	Specifies whether to use reverse query. Value options: • **true**: Query the previous page. • **false** (default): Query the next page. Note: • This parameter must be used together with **limit**. • If **page_reverse** is set to **true** and you want to query the previous page, set the value of **marker** to the value of **previous_marker**.
id	No	Array of strings	Specifies the health check ID. Multiple IDs can be queried in the format of *id=xxx&id=xxx*.
monitor_port	No	Array of integers	Specifies the port used for the health check. Multiple ports can be queried in the format of *monitor_port=xxx&monitor_port=xxx*.

Parameter	Mandatory	Type	Description
domain_name	No	Array of strings	Specifies the domain name to which HTTP requests are sent during the health check. The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter. Multiple domain names can be queried in the format of *domain_name=xxx&domain_name=xxx*.
name	No	Array of strings	Specifies the health check name. Multiple names can be queried in the format of *name=xxx&name=xxx*.
delay	No	Array of integers	Specifies the interval between health checks, in seconds. The value ranges from **1** to **50**. Multiple intervals can be queried in the format of *delay=xxx&delay=xxx*.
max_retries	No	Array of integers	Specifies the number of consecutive health checks when the health check result of a backend server changes from **OFFLINE** to **ONLINE**. The value ranges from **1** to **10**. Multiple values can be queried in the format of *max_retries=xxx&max_retries=xxx*.
admin_state_up	No	Boolean	Specifies the administrative status of the health check. The value can be **true** (health check is enabled) or **false** (health check is disabled).

Parameter	Mandatory	Type	Description
max_retries_down	No	Array of integers	Specifies the number of consecutive health checks when the health check result of a backend server changes from **ONLINE** to **OFFLINE**. The value ranges from **1** to **10**. Multiple values can be queried in the format of *max_retries_down=xxx&max_retries_down=xxx*.
timeout	No	Integer	Specifies the maximum time required for waiting for a response from the health check, in seconds.
type	No	Array of strings	Specifies the health check protocol. The value can be **TCP**, **UDP_CONNECT**, **HTTP**, **HTTPS**, **TLS**, or **GRPC**. Multiple protocols can be queried in the format of *type=xxx&type=xxx*.
expected_codes	No	Array of strings	Specifies the expected HTTP status code. This parameter will take effect only when **type** is set to **HTTP**, **HTTPS**, or **GRPC**. The value options are as follows: • A specific value, for example, 200 • A list of values that are separated with commas (,), for example, 200, 202 • A value range, for example, 200-204 The default value is **200**. Multiple status codes can be queried in the format of *expected_codes=xxx&expected_codes=xxx*.

Parameter	Mandatory	Type	Description
url_path	No	Array of strings	Specifies the HTTP request path for the health check. The value must start with a slash (/), and the default value is **/**. This parameter is available only when **type** is set to **HTTP** or **HTTPS**. Multiple paths can be queried in the format of *url_path=xxx&url_path=xxx*.
http_method	No	Array of strings	Specifies the HTTP method. The value can be **GET**, **HEAD**, or **POST**. Multiple methods can be queried in the format of *http_method=xxx&http_method=xxx*.
enterprise_project_id	No	Array of strings	Specifies the ID of the enterprise project. • If **enterprise_project_id** is not specified, resources in all enterprise projects are queried by default. Fine-grained authorization is performed. The **elb:healthmonitors:list** permission must be assigned to the user group. • If **enterprise_project_id** is specified, the value can be a specific enterprise project ID or **all_granted_eps**. If the value is a specific enterprise project ID, only resources in the enterprise project are queried. If the value is **all_granted_eps**, resources in the enterprise projects with the **elb:healthmonitors:list** permission are queried. Multiple values can be queried in the format of *enterprise_project_id=xxx&enterprise_project_id=xxx*.

Request Parameters

Table 5-480 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-481 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
page_info	**PageInfo** object	Shows pagination information.
healthmonitors	Array of **HealthMonitor** objects	Specifies the health check.

Table 5-482 PageInfo

Parameter	Type	Description
previous_marker	String	Specifies the ID of the first record in the pagination query result. When **page_reverse** is set to **true**, this parameter is used together to query resources on the previous page.
next_marker	String	Specifies the ID of the last record in the pagination query result.
current_count	Integer	Specifies the number of records.

Table 5-483 HealthMonitor

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the health check. • **true** (default) indicates that the health check is enabled. • **false** indicates that the health check is disabled.
delay	Integer	Specifies the interval between health checks, in seconds. The value ranges from **1** to **50**.
domain_name	String	Specifies the domain name that HTTP requests are sent to during the health check. The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter. The value is left blank by default, indicating that the virtual IP address of the load balancer is used as the destination address of HTTP requests. This parameter is available only when **type** is set to **HTTP** or **HTTPS**.
expected_codes	String	Specifies the expected HTTP status code. Value options: • A specific value, for example, 200 • A list of values that are separated with commas (,), for example, 200, 202 • A value range, for example, 200-204 If **type** is set to **GRPC**, the default value is **0**. If **type** is set to other protocols, the default value is **200**. This parameter will take effect only when **type** is set to **HTTP**, **HTTPS** or **GRPC**.
http_method	String	Specifies the HTTP method. The value can be **GET**, **HEAD**, or **POST**. The default value is **GET**. This parameter is available when **type** is set to **HTTP** or **HTTPS**.
id	String	Specifies the health check ID.

Parameter	Type	Description
max_retries	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **OFFLINE** to **ONLINE**. The value ranges from **1** to **10**.
max_retries_down	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **ONLINE** to **OFFLINE**. The value ranges from **1** to **10**, and the default value is **3**.
monitor_port	Integer	Specifies the port used for the health check. Value range: **1** to **65535**, or **null** (the port of a backend server will be used by default) Default value: **null**
name	String	Specifies the health check name.
pools	Array of **PoolRef** objects	Lists the IDs of backend server groups for which the health check is configured. Only one ID will be returned.
project_id	String	Specifies the project ID.
timeout	Integer	Specifies the maximum time required for waiting for a response from the health check, in seconds. It is recommended that you set the value less than that of parameter **delay**.

Parameter	Type	Description
type	String	Specifies the health check protocol. The value can be **TCP**, **UDP_CONNECT**, **HTTP**, **HTTPS**, **GRPC**, or **TLS**. Note: • If the protocol of the backend server is QUIC, the value can only be **UDP_CONNECT**. • If the protocol of the backend server is UDP, the value can only be **UDP_CONNECT**. • If the protocol of the backend server is TCP, the value can only be **TCP**, **HTTP**, or **HTTPS**. • If the protocol of the backend server is HTTP, the value can only be **TCP**, **HTTP**, **HTTPS**, **GRPC**, or **TLS**. • If the protocol of the backend server is HTTPS, the value can only be **TCP**, **HTTP**, **HTTPS**, **GRPC**, or **TLS**. • If the protocol of the backend server is GRPC, the value can only be **TCP**, **HTTP**, **HTTPS**, **GRPC**, or **TLS**. • If the protocol of the backend server is TLS, the value can only be **TCP**, **HTTP**, **HTTPS**, **GRPC**, or **TLS**.
url_path	String	Specifies the HTTP request path for the health check. The value must start with a slash (/), and the default value is **/**. The value can contain letters, digits, hyphens (-), slashes (/), periods (.), percentage signs (%), question marks (?), pound signs (#), ampersand signs (&), and the extended character set: _;~!()*[]@$^:',+. Note: This parameter is available only when **type** is set to **HTTP** or **HTTPS**.

Parameter	Type	Description
created_at	String	Specifies the time when the health check was configured. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
updated_at	String	Specifies the time when the health check was updated. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.

Table 5-484 PoolRef

Parameter	Type	Description
id	String	Specifies the ID of the backend server group.

Example Requests

Querying health checks

```
GET https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/healthmonitors
```

Example Responses

Status code: 200

Successful request.

```
{
  "healthmonitors" : [ {
    "monitor_port" : null,
    "id" : "c2b210b2-60c4-449d-91e2-9e9ea1dd7441",
    "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
    "domain_name" : null,
    "name" : "My Healthmonitor update",
    "delay" : 10,
    "max_retries" : 10,
    "pools" : [ {
```



```
      "id" : "488acc50-6bcf-423d-8f0a-0f4184f5b8a0"
    } ],
    "admin_state_up" : true,
    "timeout" : 30,
    "type" : "HTTP",
    "expected_codes" : "200",
    "url_path" : "/",
    "http_method" : "GET"
  }, {
    "monitor_port" : null,
    "id" : "cda1af03-0660-4fd2-8edf-e38c79846e08",
    "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
    "domain_name" : "akik..un.com",
    "name" : "lijunqiu",
    "delay" : 50,
    "max_retries" : 1,
    "pools" : [ {
      "id" : "ae6e45ba-be84-4074-8ac6-bc4a56484809"
    } ],
    "admin_state_up" : false,
    "timeout" : 3,
    "type" : "UDP_CONNECT",
    "expected_codes" : null,
    "url_path" : "/world",
    "http_method" : null
  } ],
  "page_info" : {
    "next_marker" : "cda1af03-0660-4fd2-8edf-e38c79846e08",
    "previous_marker" : "c2b210b2-60c4-449d-91e2-9e9ea1dd7441",
    "current_count" : 2
  },
  "request_id" : "814bc40e-8b0a-4ced-b8e5-f136c3e1df6a"
}
```


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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ListHealthMonitorsSolution {

    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);
```

```
        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ListHealthMonitorsRequest request = new ListHealthMonitorsRequest();
        try {
            ListHealthMonitorsResponse response = client.listHealthMonitors(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListHealthMonitorsRequest()
        response = client.list_health_monitors(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
```



```
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListHealthMonitorsRequest{}
    response, err := client.ListHealthMonitors(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	Successful request.

Error Codes

See **Error Codes**.

5.13.3 Viewing the Details of a Health Check

Function

This API is used to view the details of a health check.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/healthmonitors/{healthmonitor_id}

Table 5-485 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
healthmonitor_id	Yes	String	Specifies the health check ID.

Request Parameters

Table 5-486 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-487 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
healthmonitor	**HealthMonitor** object	Specifies the health check.

Table 5-488 HealthMonitor

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the health check. • **true** (default) indicates that the health check is enabled. • **false** indicates that the health check is disabled.

Parameter	Type	Description
delay	Integer	Specifies the interval between health checks, in seconds. The value ranges from **1** to **50**.
domain_name	String	Specifies the domain name that HTTP requests are sent to during the health check. The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter. The value is left blank by default, indicating that the virtual IP address of the load balancer is used as the destination address of HTTP requests. This parameter is available only when **type** is set to **HTTP** or **HTTPS**.
expected_codes	String	Specifies the expected HTTP status code. Value options: ● A specific value, for example, 200 ● A list of values that are separated with commas (,), for example, 200, 202 ● A value range, for example, 200-204 If **type** is set to **GRPC**, the default value is **0**. If **type** is set to other protocols, the default value is **200**. This parameter will take effect only when **type** is set to **HTTP**, **HTTPS** or **GRPC**.
http_method	String	Specifies the HTTP method. The value can be **GET**, **HEAD**, or **POST**. The default value is **GET**. This parameter is available when **type** is set to **HTTP** or **HTTPS**.
id	String	Specifies the health check ID.
max_retries	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **OFFLINE** to **ONLINE**. The value ranges from **1** to **10**.

Parameter	Type	Description
max_retries_down	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **ONLINE** to **OFFLINE**. The value ranges from **1** to **10**, and the default value is **3**.
monitor_port	Integer	Specifies the port used for the health check. Value range: **1** to **65535**, or **null** (the port of a backend server will be used by default) Default value: **null**
name	String	Specifies the health check name.
pools	Array of **PoolRef** objects	Lists the IDs of backend server groups for which the health check is configured. Only one ID will be returned.
project_id	String	Specifies the project ID.
timeout	Integer	Specifies the maximum time required for waiting for a response from the health check, in seconds. It is recommended that you set the value less than that of parameter **delay**.

Parameter	Type	Description
type	String	Specifies the health check protocol. The value can be **TCP**, **UDP_CONNECT**, **HTTP**, **HTTPS**, **GRPC**, or **TLS**. Note: • If the protocol of the backend server is QUIC, the value can only be **UDP_CONNECT**. • If the protocol of the backend server is UDP, the value can only be **UDP_CONNECT**. • If the protocol of the backend server is TCP, the value can only be **TCP**, **HTTP**, or **HTTPS**. • If the protocol of the backend server is HTTP, the value can only be **TCP**, **HTTP**, **HTTPS**, **GRPC**, or **TLS**. • If the protocol of the backend server is HTTPS, the value can only be **TCP**, **HTTP**, **HTTPS**, **GRPC**, or **TLS**. • If the protocol of the backend server is GRPC, the value can only be **TCP**, **HTTP**, **HTTPS**, **GRPC**, or **TLS**. • If the protocol of the backend server is TLS, the value can only be **TCP**, **HTTP**, **HTTPS**, **GRPC**, or **TLS**.
url_path	String	Specifies the HTTP request path for the health check. The value must start with a slash (/), and the default value is **/**. The value can contain letters, digits, hyphens (-), slashes (/), periods (.), percentage signs (%), question marks (?), pound signs (#), ampersand signs (&), and the extended character set: _;~!()*[]@$^:',+. Note: This parameter is available only when **type** is set to **HTTP** or **HTTPS**.

Parameter	Type	Description
created_at	String	Specifies the time when the health check was configured. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
updated_at	String	Specifies the time when the health check was updated. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.

Table 5-489 PoolRef

Parameter	Type	Description
id	String	Specifies the ID of the backend server group.

Example Requests

Querying the details of a health check

```
GET https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/healthmonitors/
c2b210b2-60c4-449d-91e2-9e9ea1dd7441
```

Example Responses

Status code: 200

Successful request.

```
{
  "healthmonitor" : {
    "monitor_port" : null,
    "id" : "c2b210b2-60c4-449d-91e2-9e9ea1dd7441",
    "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
    "domain_name" : null,
    "name" : "My Healthmonitor update",
    "delay" : 10,
    "max_retries" : 10,
```



```
  "pools" : [ {
    "id" : "488acc50-6bcf-423d-8f0a-0f4184f5b8a0"
  } ],
  "admin_state_up" : true,
  "timeout" : 30,
  "type" : "HTTP",
  "expected_codes" : "200",
  "url_path" : "/",
  "http_method" : "GET"
 },
 "request_id" : "3702e8f0-f5f0-4d35-9097-fc7160005fae"
}
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ShowHealthMonitorSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowHealthMonitorRequest request = new ShowHealthMonitorRequest();
        request.withHealthmonitorId("{healthmonitor_id}");
        try {
            ShowHealthMonitorResponse response = client.showHealthMonitor(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowHealthMonitorRequest()
        request.healthmonitor_id = "{healthmonitor_id}"
        response = client.show_health_monitor(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowHealthMonitorRequest{}
    request.HealthmonitorId = "{healthmonitor_id}"
    response, err := client.ShowHealthMonitor(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	Successful request.

Error Codes

See **Error Codes**.

5.13.4 Updating a Health Check

Function

This API is used to update a health check.

Constraints

The health check can be updated only when the provisioning status of the associated load balancer is **ACTIVE**.

Calling Method

For details, see **Calling APIs**.

URI

PUT /v3/{project_id}/elb/healthmonitors/{healthmonitor_id}

Table 5-490 Path Parameters

Parameter	Mandatory	Type	Description
healthmonitor_id	Yes	String	Specifies the health check ID.
project_id	Yes	String	Specifies the project ID.

Request Parameters

Table 5-491 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Table 5-492 Request body parameters

Parameter	Mandatory	Type	Description
healthmonitor	Yes	**UpdateHealthMonitorOption** object	Specifies the health check.

Table 5-493 UpdateHealthMonitorOption

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Specifies the administrative status of the health check. • **true** (default): Health check is enabled. • **false**: Health check is disabled.
delay	No	Integer	Specifies the interval between health checks, in seconds. The value ranges from **1** to **50**.

Parameter	Mandatory	Type	Description
domain_name	No	String	Specifies the domain name that HTTP requests are sent to during the health check. The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter. The value cannot be left blank, but can be specified as null or cannot be passed, indicating that the virtual IP address of the load balancer is used as the destination address of HTTP requests. This parameter is available only when **type** is set to **HTTP** or **HTTPS**.
expected_codes	No	String	Specifies the expected HTTP status code. This parameter will take effect only when **type** is set to **HTTP**, **HTTPS**, or **GRPC**. The value options are as follows: • A specific value, for example, 200 • A list of values that are separated with commas (,), for example, 200, 202 • A value range, for example, 200-204
http_method	No	String	Specifies the HTTP method. The value can be **GET**, **HEAD**, or **POST**. The default value is **GET**. This parameter is available when **type** is set to **HTTP** or **HTTPS**.
max_retries	No	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **OFFLINE** to **ONLINE**. The value ranges from **1** to **10**.

Parameter	Mandatory	Type	Description
max_retries_down	No	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **ONLINE** to **OFFLINE**. The value ranges from **1** to **10**.
monitor_port	No	Integer	Specifies the port used for the health check. Value range: **1** to **65535**, or **null** (the port of a backend server will be used by default)
name	No	String	Specifies the health check name.
timeout	No	Integer	Specifies the maximum time required for waiting for a response from the health check, in seconds. It is recommended that you set the value less than that of parameter **delay**.
url_path	No	String	Specifies the HTTP request path for the health check. The value must start with a slash (/), and the default value is **/**. The value can contain letters, digits, hyphens (-), slashes (/), periods (.), percentage signs (%), question marks (?), pound signs (#), ampersand signs (&), and the extended character set: _;~!()*[]@$^:',+. Note: This parameter is available only when **type** is set to **HTTP** or **HTTPS**.

Parameter	Mandatory	Type	Description
type	No	String	Specifies the health check protocol. The value can be **TCP**, **UDP_CONNECT**, **HTTP**, **HTTPS**, **GRPC**, or **TLS**. Note: • If the protocol of the backend server is QUIC, the value can only be **UDP_CONNECT**. • If the protocol of the backend server is UDP, the value can only be **UDP_CONNECT**. • If the protocol of the backend server is TCP, the value can only be **TCP**, **HTTP**, or **HTTPS**. • If the protocol of the backend server is HTTP, the value can only be **TCP**, **HTTP**, **HTTPS**, **GRPC**, or **TLS**. • If the protocol of the backend server is HTTPS, the value can only be **TCP**, **HTTP**, **HTTPS**, **GRPC**, or **TLS**. • If the protocol of the backend server is GRPC, the value can only be **TCP**, **HTTP**, **HTTPS**, **GRPC**, or **TLS**. • If the protocol of the backend server is TLS, the value can only be **TCP**, **HTTP**, **HTTPS**, **GRPC**, or **TLS**.

Response Parameters

Status code: 200

Table 5-494 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
healthmonitor	**HealthMonitor** object	Specifies the health check.

Table 5-495 HealthMonitor

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the health check. • **true** (default) indicates that the health check is enabled. • **false** indicates that the health check is disabled.
delay	Integer	Specifies the interval between health checks, in seconds. The value ranges from **1** to **50**.
domain_name	String	Specifies the domain name that HTTP requests are sent to during the health check. The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter. The value is left blank by default, indicating that the virtual IP address of the load balancer is used as the destination address of HTTP requests. This parameter is available only when **type** is set to **HTTP** or **HTTPS**.

Parameter	Type	Description
expected_codes	String	Specifies the expected HTTP status code. Value options: • A specific value, for example, 200 • A list of values that are separated with commas (,), for example, 200, 202 • A value range, for example, 200-204 If **type** is set to **GRPC**, the default value is **0**. If **type** is set to other protocols, the default value is **200**. This parameter will take effect only when **type** is set to **HTTP**, **HTTPS** or **GRPC**.
http_method	String	Specifies the HTTP method. The value can be **GET**, **HEAD**, or **POST**. The default value is **GET**. This parameter is available when **type** is set to **HTTP** or **HTTPS**.
id	String	Specifies the health check ID.
max_retries	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **OFFLINE** to **ONLINE**. The value ranges from **1** to **10**.
max_retries_down	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **ONLINE** to **OFFLINE**. The value ranges from **1** to **10**, and the default value is **3**.
monitor_port	Integer	Specifies the port used for the health check. Value range: **1** to **65535**, or **null** (the port of a backend server will be used by default) Default value: **null**
name	String	Specifies the health check name.

Parameter	Type	Description
pools	Array of **PoolRef** objects	Lists the IDs of backend server groups for which the health check is configured. Only one ID will be returned.
project_id	String	Specifies the project ID.
timeout	Integer	Specifies the maximum time required for waiting for a response from the health check, in seconds. It is recommended that you set the value less than that of parameter **delay**.
type	String	Specifies the health check protocol. The value can be **TCP**, **UDP_CONNECT**, **HTTP**, **HTTPS**, **GRPC**, or **TLS**. Note: • If the protocol of the backend server is QUIC, the value can only be **UDP_CONNECT**. • If the protocol of the backend server is UDP, the value can only be **UDP_CONNECT**. • If the protocol of the backend server is TCP, the value can only be **TCP**, **HTTP**, or **HTTPS**. • If the protocol of the backend server is HTTP, the value can only be **TCP**, **HTTP**, **HTTPS**, **GRPC**, or **TLS**. • If the protocol of the backend server is HTTPS, the value can only be **TCP**, **HTTP**, **HTTPS**, **GRPC**, or **TLS**. • If the protocol of the backend server is GRPC, the value can only be **TCP**, **HTTP**, **HTTPS**, **GRPC**, or **TLS**. • If the protocol of the backend server is TLS, the value can only be **TCP**, **HTTP**, **HTTPS**, **GRPC**, or **TLS**.

Parameter	Type	Description
url_path	String	Specifies the HTTP request path for the health check. The value must start with a slash (/), and the default value is **/**. The value can contain letters, digits, hyphens (-), slashes (/), periods (.), percentage signs (%), question marks (?), pound signs (#), ampersand signs (&), and the extended character set: _;~!()*[]@$^:',+. Note: This parameter is available only when **type** is set to **HTTP** or **HTTPS**.
created_at	String	Specifies the time when the health check was configured. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
updated_at	String	Specifies the time when the health check was updated. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.

Table 5-496 PoolRef

Parameter	Type	Description
id	String	Specifies the ID of the backend server group.

Example Requests

Modifying the interval between health checks

```
PUT https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/healthmonitors/
c2b210b2-60c4-449d-91e2-9e9ea1dd7441
```



```
{
  "healthmonitor" : {
    "name" : "My Healthmonitor update",
    "max_retries" : 10,
    "delay" : 10
  }
}
```

Example Responses

Status code: 200

Successful request.

```
{
  "request_id" : "08d6ffea-d092-4cfa-860a-e364f3bef1be",
  "healthmonitor" : {
    "monitor_port" : null,
    "id" : "c2b210b2-60c4-449d-91e2-9e9ea1dd7441",
    "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
    "domain_name" : null,
    "name" : "My Healthmonitor update",
    "delay" : 10,
    "max_retries" : 10,
    "pools" : [ {
      "id" : "488acc50-6bcf-423d-8f0a-0f4184f5b8a0"
    } ],
    "admin_state_up" : true,
    "timeout" : 30,
    "type" : "HTTP",
    "expected_codes" : "200",
    "url_path" : "/",
    "http_method" : "GET"
  }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Modifying the interval between health checks

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class UpdateHealthMonitorSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdateHealthMonitorRequest request = new UpdateHealthMonitorRequest();
        request.withHealthmonitorId("{healthmonitor_id}");
        UpdateHealthMonitorRequestBody body = new UpdateHealthMonitorRequestBody();
        UpdateHealthMonitorOption healthmonitorbody = new UpdateHealthMonitorOption();
        healthmonitorbody.withDelay(10)
            .withMaxRetries(10)
            .withName("My Healthmonitor update");
        body.withHealthmonitor(healthmonitorbody);
        request.withBody(body);
        try {
            UpdateHealthMonitorResponse response = client.updateHealthMonitor(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

Modifying the interval between health checks

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdateHealthMonitorRequest()
```



```
    request.healthmonitor_id = "{healthmonitor_id}"
    healthmonitorbody = UpdateHealthMonitorOption(
        delay=10,
        max_retries=10,
        name="My Healthmonitor update"
    )
    request.body = UpdateHealthMonitorRequestBody(
        healthmonitor=healthmonitorbody
    )
    response = client.update_health_monitor(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

Modifying the interval between health checks

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdateHealthMonitorRequest{}
    request.HealthmonitorId = "{healthmonitor_id}"
    delayHealthmonitor:= int32(10)
    maxRetriesHealthmonitor:= int32(10)
    nameHealthmonitor:= "My Healthmonitor update"
    healthmonitorbody := &model.UpdateHealthMonitorOption{
        Delay: &delayHealthmonitor,
        MaxRetries: &maxRetriesHealthmonitor,
        Name: &nameHealthmonitor,
    }
    request.Body = &model.UpdateHealthMonitorRequestBody{
        Healthmonitor: healthmonitorbody,
    }
    response, err := client.UpdateHealthMonitor(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	Successful request.

Error Codes

See **Error Codes**.

5.13.5 Deleting a Health Check

Function

This API is used to delete a health check.

Constraints

The health check can be deleted only when the provisioning status of the associated load balancer is **ACTIVE**.

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v3/{project_id}/elb/healthmonitors/{healthmonitor_id}

Table 5-497 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
healthmonitor_id	Yes	String	Specifies the health check ID.

Request Parameters

Table 5-498 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

None

Example Requests

Deleting a health check

```
DELETE https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/healthmonitors/
c2b210b2-60c4-449d-91e2-9e9ea1dd7441
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class DeleteHealthMonitorSolution {

    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);
```



```
        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteHealthMonitorRequest request = new DeleteHealthMonitorRequest();
        request.withHealthmonitorId("{healthmonitor_id}");
        try {
            DeleteHealthMonitorResponse response = client.deleteHealthMonitor(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteHealthMonitorRequest()
        request.healthmonitor_id = "{healthmonitor_id}"
        response = client.delete_health_monitor(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
```

```
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteHealthMonitorRequest{}
    request.HealthmonitorId = "{healthmonitor_id}"
    response, err := client.DeleteHealthMonitor(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	Successful request.

Error Codes

See **Error Codes**.

5.14 Forwarding Policy

5.14.1 Adding a Forwarding Policy

Function

This API is used to add a forwarding policy to a listener.

Constraints

Forwarding policies can be added to only to HTTP or HTTPS listeners.

Calling Method

For details, see **Calling APIs**.

URI

POST /v3/{project_id}/elb/l7policies

Table 5-499 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Request Parameters

Table 5-500 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Table 5-501 Request body parameters

Parameter	Mandatory	Type	Description
l7policy	Yes	**CreateL7PolicyOption** object	Specifies the forwarding policy.

Table 5-502 CreateL7PolicyOption

Parameter	Mandatory	Type	Description
action	Yes	String	Specifies where requests will be forwarded. Value options: • **REDIRECT_TO_POOL**: Requests will be forwarded to another backend server group. • **REDIRECT_TO_LISTENER**: Requests will be redirected to an HTTPS listener. • **REDIRECT_TO_URL**: Requests will be redirected to another URL. • **FIXED_RESPONSE**: A fixed response body will be returned. Note: • **REDIRECT_TO_LISTENER** has the highest priority. If requests are to be redirected to an HTTPS listener, other forwarding policies of the listener will become invalid. • If **action** is set to **REDIRECT_TO_POOL**, the listener's protocol must be HTTP, HTTPS, or TERMINATED_HTTPS. • If **action** is set to **REDIRECT_TO_LISTENER**, the listener's protocol must be HTTP.
admin_state_up	No	Boolean	Specifies the administrative status of the forwarding policy. Note: The value can only be **true**.
description	No	String	Provides supplementary information about the forwarding policy.

Parameter	Mandatory	Type	Description
listener_id	Yes	String	Specifies the ID of the listener to which the forwarding policy is added. Note: • If **action** is set to **REDIRECT_TO_POOL**, the forwarding policy can be added to an HTTP or HTTPS listener. • If **action** is set to **REDIRECT_TO_LISTENER**, the forwarding policy can be added to an HTTP listener.
name	No	String	Specifies the forwarding policy name.
position	No	Integer	Specifies the forwarding policy priority. The value cannot be updated. This parameter is unsupported. Please do not use it.

Parameter	Mandatory	Type	Description
priority	No	Integer	Specifies the forwarding policy priority. A smaller value indicates a higher priority. Value ranges: • If **action** is set to **REDIRECT_TO_LISTENER**, the priority ranges from 0 to 10,000. • If **action** is set to other values, the priority ranges from 1 to 10,000. Default value options: • If this parameter is not passed and **enhance_l7policy_enable** is set to **false**, the priority of the new forwarding policy is **1**. • If **action** is set to **REDIRECT_TO_LISTENER**, the priority of the new forwarding policy is **0**. • If **action** is set to other values, the priority of the new forwarding policy will be a sum of 1 and the highest priority of existing forwarding policy in the same listener by default. – If no forwarding policies exist, the priority of the new forwarding policy will be **1** by default. – If the highest priority of existing forwarding policies is the maximum value (10,000), the forwarding policy will fail to be created because the final priority for creating the forwarding policy is the sum of 1 and 10,000, which exceeds the maximum value. In this case, specify a value or adjust the priorities of

Parameter	Mandatory	Type	Description
			existing forwarding policies. Note: • The value must be unique for forwarding policies of the same listener. • This parameter takes effect only when **enhance_l7policy_enable** is set to **true**. If this parameter is passed and **enhance_l7policy_enable** is set to **false**, an error will be returned. • If **enhance_l7policy_enable** is not enabled, forwarding policies are automatically prioritized based on the original policy sorting logic. The priorities of domain names are independent from each other. For the same domain name, the priorities are sorted in the order of exact match (**EQUAL_TO**), prefix match (**STARTS_WITH**), and regular expression match (**REGEX**). If the matching types are the same, the longer the path is, the higher the priority is. If a forwarding policy contains only a domain name without a path specified, the path is **/**, and prefix match is used by default. This parameter is supported by forwarding policies of shared load balancers.
project_id	No	String	Specifies the ID of the project where the forwarding policy is used.

Parameter	Mandatory	Type	Description
redirect_listener_id	No	String	Specifies the ID of the listener to which requests are redirected. Note: • This parameter is mandatory when **action** is set to **REDIRECT_TO_LISTENER**. • The listener's protocol must be **HTTPS** or **TERMINATED_HTTPS**. • A listener added to another load balancer is not allowed. • This parameter cannot be passed in the API for adding or updating a forwarding policy if **action** is set to **REDIRECT_TO_POOL**. • This parameter is unsupported for shared load balancers.
redirect_pool_id	No	String	Specifies the ID of the backend server group to which the requests are forwarded. Note: • This parameter is valid only when **action** is set to **REDIRECT_TO_POOL**. • If this parameter is specified when **action** is set to **REDIRECT_TO_LISTENER**, an error will be reported.
redirect_url	No	String	Specifies the URL to which requests are forwarded. Format: *protocol://host:port/path?query*

Parameter	Mandatory	Type	Description
redirect_url_config	No	CreateRedirectUrlConfig object	Specifies the URL to which requests are forwarded. Note: • This parameter will take effect only when advanced forwarding is enabled (**enhance_l7policy_enable** is set to **true**). If it is passed when **enhance_l7policy_enable** is set to **false**, an error will be returned. • This parameter is mandatory when **action** is set to **REDIRECT_TO_URL**. It cannot be specified if the value of **action** is not **REDIRECT_TO_URL**. • For shared load balancers, this parameter is unsupported. If it is passed, an error will be returned. • At least one of the four parameters (**protocol**, **host**, **port**, and **path**) must be passed, or their values cannot be set to **${xxx}** at the same time. **${xxx}** indicates that the value in the request will be used. For example, **${host}** indicates the host in the URL to be redirected. • The values of **protocol** and **port** cannot be the same as those of the associated listener, and either **host** or **path** must be passed or their values cannot be **${xxx}** at the same time. Value format: *protocol://host:port/path?query*

Parameter	Mandatory	Type	Description
redirect_pools_config	No	Array of **CreateRedirectPoolsConfig** objects	Specifies the backend server groups that the requests are forwarded to. Note: A maximum of 5 backend server groups can be configured for a forwarding policy.
redirect_pools_sticky_session_config	No	**CreateRedirectPoolsStickySessionConfig** object	Specifies whether to enable sticky session for backend server groups configured for a forwarding policy. The load balancer generates a cookie after it receives a request from a client. All subsequent requests with the same cookie are routed to the same backend server groups. This parameter is unsupported for shared load balancers. If it is passed, an error will be returned.
fixed_response_config	No	**CreateFixtedResponseConfig** object	Specifies the configuration of the page that will be returned. Note: • This parameter will take effect when **enhance_l7policy_enable** is set to **true**. If this parameter is passed and **enhance_l7policy_enable** is set to **false**, an error will be returned. • This parameter is mandatory when **action** is set to **FIXED_RESPONSE**. It cannot be specified if the value of **action** is not **FIXED_RESPONSE**. • For shared load balancers, this parameter is unsupported. If it is passed, an error will be returned.

Parameter	Mandatory	Type	Description
redirect_pools_extend_config	No	CreateRedirectPoolsExtendConfig object	Specifies the backend server group that requests are forwarded to. Note: This parameter takes effect only when **action** is set to **REDIRECT_TO_POOL**.
rules	No	Array of CreateL7PolicyRuleOption objects	Lists the forwarding rules in the forwarding policy. Note: • Each list can contain a maximum of 10 forwarding rules (if **conditions** is specified, a condition is considered as a rule). If **type** is set to **HOST_NAME**, **PATH**, **METHOD**, or **SOURCE_IP**, only one forwarding rule can be created for each type. • The entire list will be replaced if you update it. • If the action of **17policy** is set to **Redirect to another listener**, **17rule** cannot be created.

Table 5-503 CreateRedirectUrlConfig

Parameter	Mandatory	Type	Description
protocol	No	String	Specifies the protocol for redirection. The value can be **HTTP**, **HTTPS**, or **${protocol}**. The default value is **${protocol}**, indicating that the protocol of the request will be used.

Parameter	Mandatory	Type	Description
host	No	String	Specifies the name of the host that requests are redirected to. The value can contain only letters, digits, hyphens (-), and periods (.) and must start with a letter or digit. The default value is **${host}**, indicating that the host of the request will be used.
port	No	String	Specifies the port that requests are redirected to. The default value is **${port}**, indicating that the port of the request will be used.
path	No	String	Specifies the path that requests are redirected to. The value can contain only letters, digits, and special characters: _~';@^-%#&$.* +?,=!:|\/()[]{} and must start with a slash (/). $1, $2, $3, and all the way to $9 match the wildcard asterisk (*) in the request URL. The default value is **${path}**, indicating that the path of the request will be used.

Parameter	Mandatory	Type	Description
query	No	String	Specifies the query string set in the URL for redirection. The value is case-sensitive and can contain only letters, digits, and special characters: !$&'()* +,-./:;=?@^_`. $1, $2, $3, and all the way to $9 match the wildcard asterisk (*) in the request URL. The default value is **${query}**, indicating that the query string of the request will be used. For example, in the URL **https://www.example.com:8080/elb?type=loadbalancer**, **${query}** indicates **type=loadbalancer**. If this parameter is set to **${query}&name=my_name**, the URL will be redirected to **https://www.example.com:8080/elb?type=loadbalancer&name=my_name**.
status_code	Yes	String	Specifies the status code returned after the requests are redirected. The value can be **301**, **302**, **303**, **307**, or **308**.
insert_headers_config	No	**CreateInsertHeadersConfig** object	Specifies the headers you want to write into the request that matches the forwarding rule.
remove_headers_config	No	**CreateRemoveHeadersConfig** object	Specifies the headers you want to remove from the request that matches the forwarding rule.

Table 5-504 CreateRedirectPoolsConfig

Parameter	Mandatory	Type	Description
pool_id	Yes	String	Specifies the ID of the backend server group.

Parameter	Mandatory	Type	Description
weight	No	String	Specifies the weight of the backend server group. The value ranges from **1** (default) to **100**. Requests are routed to backend server groups based on their weights. Backend server groups with higher weights receive proportionately more requests. No requests will be routed to a backend server group with a weight of 0.

Table 5-505 CreateRedirectPoolsStickySessionConfig

Parameter	Mandatory	Type	Description
enable	No	Boolean	Specifies whether to enable sticky session for backend server groups configured in a forwarding policy. The default value is **false**, indicating that sticky session is disabled.
timeout	No	Integer	Specifies the duration that a session persists. The value ranges from **1** to **1440** (default), in minutes.

Table 5-506 CreateFixtedResponseConfig

Parameter	Mandatory	Type	Description
status_code	Yes	String	Specifies the fixed HTTP status code configured in the forwarding rule. The value can be any integer in the range of 200–299, 400–499, or 500–599.

Parameter	Mandatory	Type	Description
content_type	No	String	Specifies the format of the response body. The value can be **text/plain**, **text/css**, **text/html**, **application/javascript**, or **application/json**. The default value is **text/plain**.
message_body	No	String	Specifies the content of the response message body.
insert_headers_config	No	**CreateInsertHeadersConfig** object	Specifies the headers you want to write into the request that matches the forwarding rule.
remove_headers_config	No	**CreateRemoveHeadersConfig** object	Specifies the headers you want to remove from the request that matches the forwarding rule.
traffic_limit_config	No	**CreateTrafficLimitConfig** object	Specifies how requests are limited.

Table 5-507 CreateRedirectPoolsExtendConfig

Parameter	Mandatory	Type	Description
rewrite_url_enable	No	Boolean	Specifies whether to set **rewrite_url_enable** to **true**.
rewrite_url_config	No	**CreateRewriteUrlConfig** object	Specifies the URL for the backend server group that requests are forwarded to. This parameter takes effect only when **action** is set to **REDIRECT_TO_POOL**.
insert_headers_config	No	**CreateInsertHeadersConfig** object	Specifies the headers you want to write into the request that matches the forwarding rule.
remove_headers_config	No	**CreateRemoveHeadersConfig** object	Specifies the headers you want to remove from the request that matches the forwarding rule.

Parameter	Mandatory	Type	Description
traffic_limit_config	No	CreateTrafficLimitConfig object	Specifies how requests are limited.
cors_config	No	CreateCorsConfig object	Specifies the CORS configurations.

Table 5-508 CreateRewriteUrlConfig

Parameter	Mandatory	Type	Description
host	No	String	Specifies the domain name of the host that requests are redirected to. The domain name can contain only letters, digits, hyphens (-), and periods (.), and must start with a letter or digit. The default value is **${host}**, indicating that the host of the request will be used.
path	No	String	Specifies the path that requests are redirected to. The default value is **${path}**, indicating that the path of the request will be used. The value can contain only letters, digits, and special characters: _~';@^-%#&$.+?,=!:|/() and must start with a slash (/). $1, $2, $3, and all the way to $9 match the wildcard asterisk (*) in the request URL. If the number of regular expression match groups is less than the specified number, **${path}** is empty. If the dollar sign ($) is followed by a letter, the matching result is empty until the next special character appears, for example, **$abc#123**, and the matching result is **#123**. If the dollar sign ($) is followed by a special character, for example, **$#**, the matching result is **$#**.

Parameter	Mandatory	Type	Description
query	No	String	Specifies the query string set in the URL for redirection. The value is case-sensitive and can contain only letters, digits, and special characters: !$&'() *+,-./:;=?@^_`. $1, $2, $3, and all the way to $9 match the wildcard asterisk ()* in the request URL. The default value is **${query}**, indicating that the query string of the request will be used. If the number of regular expression match groups is less than the specified number, **${path}** is empty. If the dollar sign ($) is followed by a letter, the matching result is empty until the next special character appears, for example, **$abc#123**, and the matching result is **#123**. If the dollar sign ($) is followed by a special character, for example, **$#**, the matching result is **$#**.

Table 5-509 CreateInsertHeadersConfig

Parameter	Mandatory	Type	Description
configs	Yes	Array of **CreateInsertHeaderConfig** objects	Specifies the headers you want to write into the request that matches the forwarding rule.

Table 5-510 CreateInsertHeaderConfig

Parameter	Mandatory	Type	Description
key	Yes	String	Specifies the key of the header you want to write into the request that matches the forwarding rule. The value is a string of 1 to 40 case-insensitive characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. The key cannot be the following: connection, upgrade, content-length, transfer-encoding, keep-alive, te, host, cookie, remoteip, authority, x-forwarded-host, x-forwarded-for, x-forwarded-for-port, x-forwarded-tls-certificate-id, x-forwarded-tls-protocol, x-forwarded-tls-cipher, x-forwarded-elb-ip, x-forwarded-port, x-forwarded-elb-id, x-forwarded-elb-vip, x-real-ip, x-forwarded-proto, x-nuwa-trace-ne-in, or x-nuwa-trace-ne-out.
value_type	Yes	String	Specifies the value type of the header. The value can be **USER_DEFINED**, **REFERENCE_HEADER**, or **SYSTEM_DEFINED**.

Parameter	Mandatory	Type	Description
value	Yes	String	Specifies the value of the header. If **value_type** is set to **SYSTEM_DEFINED**, the value can be **CLIENT-PORT**, **CLIENT-IP**, **ELB-PROTOCOL**, **ELB-ID**, **ELB-PORT**, **ELB-EIP**, or **ELB-VIP**. The value can contain 1 to 128 characters. ASCII codes 32 through 127 printable characters, asterisk (*), and question mark (?) are also supported. The value cannot start or end with a space.

Table 5-511 CreateRemoveHeadersConfig

Parameter	Mandatory	Type	Description
configs	Yes	Array of **CreateRemoveHeaderConfig** objects	Specifies the headers you want to remove from the request that matches the forwarding rule.

Table 5-512 CreateRemoveHeaderConfig

Parameter	Mandatory	Type	Description
key	Yes	String	Specifies the key of the header you want to remove from the request that matches the forwarding rule. The value is a string of 1 to 40 case-insensitive characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. The key cannot be the following: connection, upgrade, content-length, transfer-encoding, keep-alive, te, host, cookie, remoteip, authority, x-forwarded-host, x-forwarded-for, x-forwarded-for-port, x-forwarded-tls-certificate-id, x-forwarded-tls-protocol, x-forwarded-tls-cipher, x-forwarded-elb-ip, x-forwarded-port, x-forwarded-elb-id, x-forwarded-elb-vip, x-real-ip, x-forwarded-proto, x-nuwa-trace-ne-in, or x-nuwa-trace-ne-out.

Table 5-513 CreateTrafficLimitConfig

Parameter	Mandatory	Type	Description
qps	No	Integer	Specifies the maximum number of queries per second (QPS). The value ranges from **0** to **100000**. **0** indicates that QPS is not limited.

Parameter	Mandatory	Type	Description
per_source_ip_qps	No	Integer	Specifies the maximum number of queries per second (QPS) from a source IP address. This parameter is not available for QUIC listeners. The value can be **0** or **null**. The value ranges from **0** to **100000**. **0** indicates that QPS is not limited. If **qps** is not set to **0**, **per_source_ip_qps** must be specified a smaller value than **qps**.
burst	No	Integer	Specifies the maximum number of queries per second (QPS) from a source IP address. The value ranges from **0** to **100000**. If the number of requests exceeds the value specified for **qps** but not reaches the value specified for **burst**, 503 status code will not be returned.

Table 5-514 CreateCorsConfig

Parameter	Mandatory	Type	Description
allow_origin	No	Array of strings	Specifies the origins that are allowed to access cross-origin resources through a browser. The origin can be a wildcard (*) or one or more URLs. Constraints: • Each URL must start with **http://** or **https://**, followed by a valid domain name or level-1 wildcard domain name, for example, http://*.test.abc.example.com. • It is optional to include a port number (ranging from 1 to 65535) in the URL.

Parameter	Mandatory	Type	Description
allow_methods	No	Array of strings	Specifies the HTTP methods that the specified URLs can use to access cross-origin resources.
allow_headers	No	Array of strings	Specifies the request headers that can be carried in CORS requests.
expose_headers	No	Array of strings	Specifies the headers that can be exposed.
allow_credentials	No	Boolean	Specifies whether to allow credentials in CORS requests. Value options: • **true**: Credentials are allowed. • **false**: Credentials are not allowed.
max_age	No	Long	Specifies the maximum duration a preflight request can be cached, in seconds. Value range: -1 to 172800

Table 5-515 CreateL7PolicyRuleOption

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Specifies the administrative status of the forwarding rule. The value can only be **true**.

Parameter	Mandatory	Type	Description
type	Yes	String	Specifies the type of the forwarding rule. Value options: • **HOST_NAME**: A domain name will be used for matching. • **PATH**: A URL will be used for matching. • **METHOD**: An HTTP request method will be used for matching. • **HEADER**: The request header will be used for matching. • **QUERY_STRING**: A query string will be used for matching. • **SOURCE_IP**: The source IP address will be used for matching. • **COOKIE**: The cookie will be used for matching. Note: If **type** is set to **HOST_NAME**, **PATH**, **METHOD**, or **SOURCE_IP**, only one forwarding rule can be created for each type. If **type** is set to **HEADER** and **QUERY_STRING**, multiple forwarding rules can be created for each type.

Parameter	Mandatory	Type	Description
compare_type	Yes	String	Specifies how requests are matched with the forwarding rule. Value options: • **EQUAL_TO**: exact match. • **REGEX**: regular expression match • **STARTS_WITH**: prefix match Note: • If **type** is set to **HOST_NAME**, the value can only be **EQUAL_TO**, and asterisks (*) can be used as wildcard characters. • If **type** is set to **PATH**, the value can be **REGEX**, **STARTS_WITH**, or **EQUAL_TO**. • If **type** is set to **METHOD** or **SOURCE_IP**, the value can only be **EQUAL_TO**. • If **type** is set to **HEADER** or **QUERY_STRING**, the value can only be **EQUAL_TO**, asterisks (*) and question marks (?) can be used as wildcard characters.
invert	No	Boolean	Specifies whether reverse matching is supported. Value range: **true** or **false** Default value: **false** This parameter is unsupported. Please do not use it.
key	No	String	Specifies the key of the match item. For example, if an HTTP header is used for matching, **key** is the name of the HTTP header parameter. This parameter is unsupported. Please do not use it.

Parameter	Mandatory	Type	Description
value	Yes	String	Specifies the value of the match item. For example, if a domain name is used for matching, **value** is the domain name. Note: • This parameter will take effect only when **conditions** is left blank. • If **type** is set to **HOST_NAME**, the value can contain letters, digits, hyphens (-), and periods (.) and must start with a letter, digit, or *. If you want to use a wildcard domain name, enter * as the leftmost label of the domain name. • If **type** is set to **PATH** and **compare_type** to **STARTS_WITH** or **EQUAL_TO**, the value must start with a slash (/) and can contain only letters, digits, and special characters: _~';@^-%#&$.* +?,=!:|\/()[]{} • If **type** is set to **METHOD**, **SOURCE_IP**, **HEADER**, or **QUERY_STRING**, this parameter will not take effect, and **conditions** will be used to specify the key and value.

Parameter	Mandatory	Type	Description
conditions	No	Array of **CreateRuleCondition** objects	Specifies the conditions contained in a forwarding rule. Note: • This parameter will take effect when **enhance_l7policy_enable** is set to **true**. • If **conditions** is specified, **key** and **value** will not take effect. • The keys in the list must be the same, whereas each value must be unique.

Table 5-516 CreateRuleCondition

Parameter	Mandatory	Type	Description
key	No	String	Specifies the key of match item. Note: • All keys in the conditions list in the same rule must be the same. • If **type** is set to **HOST_NAME**, **PATH**, **METHOD**, or **SOURCE_IP**, this parameter is an empty string. • If **type** is set to **HEADER**, **key** indicates the name of the HTTP header parameter, and **value** indicates the value of the request header parameter. The value can contain 1 to 40 characters, including letters, digits, hyphens (-), and underscores (_). • If **type** is set to **QUERY_STRING**, **key** indicates the name of the query parameter, and **value** indicates the value of the query parameter. The key is case sensitive and can contain 1 to 128 characters. Spaces, square brackets ([ ]), curly brackets ({ }), angle brackets (< >), backslashes (), double quotation marks (" "), pound signs (#), ampersands (&), vertical bars (|), percent signs (%), and tildes (~) are not supported.

Parameter	Mandatory	Type	Description
value	Yes	String	Specifies the value of the match item. Note: • The key of each condition in a forwarding policy must be the same. • The value of each condition in a forwarding policy must be unique. Value ranges: • If **type** is set to **HOST_NAME**, **key** is left blank, **value** indicates the domain name, which can contain 1 to 128 characters, including letters, digits, hyphens (-), periods (.), and asterisks (*), and must start with a letter, digit, or asterisk (*). If you want to use a wildcard domain name, enter an asterisk (*) as the leftmost label of the domain name. • If **type** is set to **PATH**, **key** is left blank, **value** indicates the request path, which can contain 1 to 128 characters. If **compare_type** is set to **STARTS_WITH** or **EQUAL_TO** for the forwarding rule, the value must start with a slash (/) and can contain only letters, digits, and special characters: _~';@^-%#&$.*+?,=!:|/()[]{} • If **type** is set to **HEADER**, **key** indicates the name of the HTTP header parameter and **value** indicates the value of the HTTP header parameter. The value can contain 1 to 128 characters. Asterisks (*) and question marks (?) are allowed, but spaces and double

Parameter	Mandatory	Type	Description
			quotation marks are not allowed. An asterisk can match zero or more characters, and a question mark can match 1 character. • If **type** is set to **QUERY_STRING**, **key** indicates the name of the query parameter and **value** indicates the value of the query parameter. The value is case sensitive and can contain 1 to 128 characters. Spaces, square brackets ([ ]), curly brackets ({ }), angle brackets (< >), backslashes (), double quotation marks (" "), pound signs (#), ampersands (&), vertical bars (|), percent signs (%), and tildes (~) are not supported. Asterisks (*) and question marks (?) are allowed. An asterisk can match zero or more characters, and a question mark can match 1 character. • If **type** is set to **METHOD**, **key** is left blank, **value** indicates the HTTP method. The value can be **GET**, **PUT**, **POST**, **DELETE**, **PATCH**, **HEAD**, or **OPTIONS**. • If **type** is set to **SOURCE_IP**, **key** is left blank, **value** indicates the source IP address of the request. The value is an IPv4 or IPv6 CIDR block, for example, 192.168.0.2/32 or 2049::49/64.

Response Parameters

Status code: 201

Table 5-517 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
l7policy	**L7Policy** object	Specifies the forwarding policy.

Table 5-518 L7Policy

Parameter	Type	Description
action	String	Specifies where requests will be forwarded. Value options: • **REDIRECT_TO_POOL**: Requests will be forwarded to another backend server group. • **REDIRECT_TO_LISTENER**: Requests will be redirected to an HTTPS listener. • **REDIRECT_TO_URL**: Requests will be redirected to another URL. • **FIXED_RESPONSE**: A fixed response body will be returned. Note: • **REDIRECT_TO_LISTENER** has the highest priority. If requests are to be redirected to an HTTPS listener, other forwarding policies of the listener will become invalid. • If **action** is set to **REDIRECT_TO_POOL**, the listener's protocol must be HTTP, HTTPS, or TERMINATED_HTTPS. • If **action** is set to **REDIRECT_TO_LISTENER**, the listener's protocol must be HTTP.
admin_state_up	Boolean	Specifies the administrative status of the forwarding policy. Note: The value can only be **true**.
description	String	Provides supplementary information about the forwarding policy.
id	String	Specifies the forwarding policy ID.

Parameter	Type	Description
listener_id	String	Specifies the ID of the listener to which the forwarding policy is added.
name	String	Specifies the forwarding policy name.
position	Integer	Specifies the forwarding policy priority. This parameter cannot be updated. This parameter is unsupported. Please do not use it.

Parameter	Type	Description
priority	Integer	Specifies the forwarding policy priority. A smaller value indicates a higher priority. Value ranges: • If **action** is set to **REDIRECT_TO_LISTENER**, the priority ranges from 0 to 10,000. • If **action** is set to other values, the priority ranges from 1 to 10,000. Default value options: • If this parameter is not passed and **enhance_l7policy_enable** is set to **false**, the priority of the new forwarding policy is **1**. • If **action** is set to **REDIRECT_TO_LISTENER**, the priority of the new forwarding policy is **0**. • If **action** is set to other values, the priority of the new forwarding policy will be a sum of 1 and the highest priority of existing forwarding policy in the same listener by default. – If no forwarding policies exist, the priority of the new forwarding policy will be **1** by default. – If the highest priority of existing forwarding policies is the maximum value (10,000), the forwarding policy will fail to be created because the final priority for creating the forwarding policy is the sum of 1 and 10,000, which exceeds the maximum value. In this case, specify a value or adjust the priorities of existing forwarding policies. Note: • The value must be unique for forwarding policies of the same listener. • This parameter takes effect only when **enhance_l7policy_enable** is

Parameter	Type	Description
		set to **true**. If this parameter is passed and **enhance_l7policy_enable** is set to **false**, an error will be returned. • If **enhance_l7policy_enable** is not enabled, forwarding policies are automatically prioritized based on the original policy sorting logic. The priorities of domain names are independent from each other. For the same domain name, the priorities are sorted in the order of exact match (**EQUAL_TO**), prefix match (**STARTS_WITH**), and regular expression match (**REGEX**). If the matching types are the same, the longer the path is, the higher the priority is. If a forwarding policy contains only a domain name without a path specified, the path is **/**, and prefix match is used by default. This parameter is supported by forwarding policies of shared load balancers.
project_id	String	Specifies the project ID of the forwarding policy.
provisioning_status	String	Specifies the provisioning status of the forwarding policy. The value can be **ACTIVE** or **ERROR**. • **ACTIVE** (default): The forwarding policy is provisioned successfully. • **ERROR**: Another forwarding policy of the same listener has the same forwarding rule.
redirect_pool_id	String	Specifies the ID of the backend server group to which the requests are forwarded. Note: This parameter is valid only when **action** is set to **REDIRECT_TO_POOL**.

Parameter	Type	Description
redirect_listener_id	String	Specifies the ID of the listener to which requests are redirected. Note: • This parameter is mandatory when **action** is set to **REDIRECT_TO_LISTENER**. • The listener's protocol must be **HTTPS** or **TERMINATED_HTTPS**. • A listener added to another load balancer is not allowed. • This parameter cannot be passed in the API for adding or updating a forwarding policy if **action** is set to **REDIRECT_TO_POOL**.
redirect_url	String	Specifies the URL to which requests are forwarded. Format: *protocol://host:port/path?query* This parameter is unsupported. Please do not use it.
rules	Array of **RuleRef** objects	Lists the forwarding rules in the forwarding policy.

Parameter	Type	Description
redirect_url_config	**RedirectUrlConfig** object	Specifies the URL to which requests are forwarded. Note: • This parameter will take effect only when advanced forwarding is enabled (**enhance_l7policy_enable** is set to **true**). If it is passed when **enhance_l7policy_enable** is set to **false**, an error will be returned. • This parameter is mandatory when **action** is set to **REDIRECT_TO_URL**. It cannot be specified if the value of **action** is not **REDIRECT_TO_URL**. • For shared load balancers, this parameter is unsupported. If it is passed, an error will be returned. • At least one of the four parameters (**protocol**, **host**, **port**, and **path**) must be passed, or their values cannot be set to **${xxx}** at the same time. **${xxx}** indicates that the value in the request will be used. For example, **${host}** indicates the host in the URL to be redirected. • The values of **protocol** and **port** cannot be the same as those of the associated listener, and either **host** or **path** must be passed or their values cannot be **${xxx}** at the same time. Value format: *protocol://host:port/path?query*
redirect_pools_config	Array of **RedirectPoolsConfig** objects	Specifies the backend server groups that the requests are forwarded to. Note: A maximum of 5 backend server groups can be configured for a forwarding policy.

Parameter	Type	Description
redirect_pools_sticky_session_config	**RedirectPoolsStickySessionConfig** object	Specifies whether to enable sticky session for backend server groups configured for a forwarding policy. The load balancer generates a cookie after it receives a request from a client. All subsequent requests with the same cookie are routed to the same backend server groups. This parameter is unsupported for shared load balancers. If it is passed, an error will be returned.
redirect_pools_extend_config	**RedirectPoolsExtendConfig** object	Specifies the backend server group that requests are forwarded to. Note: This parameter takes effect only when **action** is set to **REDIRECT_TO_POOL**.
fixed_response_config	**FixtedResponseConfig** object	Specifies the configuration of the page that will be returned. Note: • This parameter will take effect when **enhance_l7policy_enable** is set to **true**. If this parameter is passed and **enhance_l7policy_enable** is set to **false**, an error will be returned. • This parameter is mandatory when **action** is set to **FIXED_RESPONSE**. It cannot be specified if the value of **action** is not **FIXED_RESPONSE**. • For shared load balancers, this parameter is unsupported. If it is passed, an error will be returned.
created_at	String	Specifies the time when the forwarding policy was added. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.

Parameter	Type	Description
updated_at	String	Specifies the time when the forwarding policy was updated. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
enterprise_project_id	String	Specifies the ID of the enterprise project.

Table 5-519 RuleRef

Parameter	Type	Description
id	String	Specifies the forwarding rule ID.

Table 5-520 RedirectUrlConfig

Parameter	Type	Description
protocol	String	Specifies the protocol for redirection. The value can be **HTTP**, **HTTPS**, or **${protocol}**. **${protocol}** indicates that the protocol of the request will be used.
host	String	Specifies the name of the host that requests are redirected to. The value can contain only letters, digits, hyphens (-), and periods (.) and must start with a letter or digit. The default value is **${host}**, indicating that the host of the request will be used.
port	String	Specifies the port that requests are redirected to. The default value is **${port}**, indicating that the port of the request will be used.

Parameter	Type	Description
path	String	Specifies the path that requests are redirected to. The value can contain only letters, digits, and special characters: _~';@^-%#&$.*+?,=!:|\/()[]{} and must start with a slash (/). $1, $2, $3, and all the way to $9 match the wildcard asterisk (*) in the request URL. The default value is **${path}**, indicating that the path of the request will be used.
query	String	Specifies the query string set in the URL for redirection. The value is case-sensitive and can contain only letters, digits, and special characters: !$&'()*+,-./:;=?@^_`. $1, $2, $3, and all the way to $9 match the wildcard asterisk (*) in the request URL. The default value is **${query}**, indicating that the query string of the request will be used. For example, in the URL **https://www.example.com:8080/elb?type=loadbalancer**, **${query}** indicates **type=loadbalancer**. If this parameter is set to **${query}&name=my_name**, the URL will be redirected to **https://www.example.com:8080/elb?type=loadbalancer&name=my_name**.
status_code	String	Specifies the status code returned after the requests are redirected. The value can be **301**, **302**, **303**, **307**, or **308**.
insert_headers_config	**InsertHeadersConfig** object	Specifies the headers you want to write into the request that matches the forwarding rule.
remove_headers_config	**RemoveHeadersConfig** object	Specifies the headers you want to remove from the request that matches the forwarding rule.

Table 5-521 RedirectPoolsConfig

Parameter	Type	Description
pool_id	String	Specifies the ID of the backend server group.
weight	Integer	Specifies the weight of the backend server group. The value ranges from **0** to **100**. Requests are routed to backend server groups based on their weights. Backend server groups with higher weights receive proportionately more requests. No requests will be routed to a backend server group with a weight of 0.

Table 5-522 RedirectPoolsStickySessionConfig

Parameter	Type	Description
enable	Boolean	Specifies whether to enable sticky session for backend server groups configured in a forwarding policy. The default value is **false**, indicating that sticky session is disabled.
timeout	Integer	Specifies the duration that a session persists. The value ranges from **1** to **1440** (default), in minutes.

Table 5-523 RedirectPoolsExtendConfig

Parameter	Type	Description
rewrite_url_enable	Boolean	Specifies whether to set **rewrite_url_enable** to **true**.
rewrite_url_config	**RewriteUrlConfig** object	Specifies the URL for the backend server group that requests are forwarded to. This parameter takes effect only when **action** is set to **REDIRECT_TO_POOL**.
insert_headers_config	**InsertHeadersConfig** object	Specifies the headers you want to write into the request that matches the forwarding rule.

Parameter	Type	Description
remove_headers_config	**RemoveHeadersConfig** object	Specifies the headers you want to remove from the request that matches the forwarding rule.
traffic_limit_config	**TrafficLimitConfig** object	Specifies how requests are limited.
cors_config	**CorsConfig** object	Specifies the CORS configurations.

Table 5-524 RewriteUrlConfig

Parameter	Type	Description
host	String	Specifies the domain name of the host that requests are redirected to. The domain name can contain only letters, digits, hyphens (-), and periods (.), and must start with a letter or digit. The default value is **${host}**, indicating that the host of the request will be used.
path	String	Specifies the path that requests are redirected to. The default value is **${path}**, indicating that the path of the request will be used. The value can contain only letters, digits, and special characters: _~';@^-%#&$.+?,=!:|/() and must start with a slash (/). $1, $2, $3, and all the way to $9 match the wildcard asterisk (*) in the request URL. If the number of regular expression match groups is less than the specified number, **${path}** is empty. If the dollar sign ($) is followed by a letter, the matching result is empty until the next special character appears, for example, **$abc#123**, and the matching result is **#123**. If the dollar sign ($) is followed by a special character, for example, **$#**, the matching result is **$#**.

Parameter	Type	Description
query	String	Specifies the query string set in the URL for redirection. The value is case-sensitive and can contain only letters, digits, and special characters: !$&'()*+,-./:;=?@^_`. *$1, $2, $3, and all the way to $9 match the wildcard asterisk ()* in the request URL. The default value is **${query}**, indicating that the query string of the request will be used. If the number of regular expression match groups is less than the specified number, **${path}** is empty. If the dollar sign ($) is followed by a letter, the matching result is empty until the next special character appears, for example, **$abc#123**, and the matching result is **#123**. If the dollar sign ($) is followed by a special character, for example, **$#**, the matching result is **$#**.

Table 5-525 CorsConfig

Parameter	Type	Description
allow_origin	Array of strings	Specifies the origins that are allowed to access cross-origin resources through a browser. The origin can be a wildcard (*) or one or more URLs. Constraints: • Each URL must start with **http://** or **https://**, followed by a valid domain name or level-1 wildcard domain name, for example, http://*.test.abc.example.com. • It is optional to include a port number (ranging from 1 to 65535) in the URL.
allow_methods	Array of strings	Specifies the HTTP methods that the specified URLs can use to access cross-origin resources.
allow_headers	Array of strings	Specifies the request headers that can be carried in CORS requests.
expose_headers	Array of strings	Specifies the headers that can be exposed.

Parameter	Type	Description
allow_credentials	Boolean	Specifies whether to allow credentials in CORS requests. Value options: • **true**: Credentials are allowed. • **false**: Credentials are not allowed.
max_age	Long	Specifies the maximum duration a preflight request can be cached, in seconds. Value range: -1 to 172800

Table 5-526 FixtedResponseConfig

Parameter	Type	Description
status_code	String	Specifies the HTTP status code configured in the forwarding policy. The value can be any integer in the range of 200–299, 400–499, or 500–599.
content_type	String	Specifies the format of the response body. The value can be **text/plain**, **text/css**, **text/html**, **application/javascript**, or **application/json**.
message_body	String	Specifies the content of the response message body.
insert_headers_config	**InsertHeadersConfig** object	Specifies the headers you want to write into the request that matches the forwarding rule.
remove_headers_config	**RemoveHeadersConfig** object	Specifies the headers you want to remove from the request that matches the forwarding rule.
traffic_limit_config	**TrafficLimitConfig** object	Specifies how requests are limited.

Table 5-527 InsertHeadersConfig

Parameter	Type	Description
configs	Array of **InsertHeaderConfig** objects	Specifies the headers you want to write into the request that matches the forwarding rule.

Table 5-528 InsertHeaderConfig

Parameter	Type	Description
key	String	Specifies the key of the header you want to write into the request that matches the forwarding rule. The value is a string of 1 to 40 case-insensitive characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. The key cannot be the following: connection, upgrade, content-length, transfer-encoding, keep-alive, te, host, cookie, remoteip, authority, x-forwarded-host, x-forwarded-for, x-forwarded-for-port, x-forwarded-tls-certificate-id, x-forwarded-tls-protocol, x-forwarded-tls-cipher, x-forwarded-elb-ip, x-forwarded-port, x-forwarded-elb-id, x-forwarded-elb-vip, x-real-ip, x-forwarded-proto, x-nuwa-trace-ne-in, or x-nuwa-trace-ne-out.
value_type	String	Specifies the value type of the header. The value can be **USER_DEFINED**, **REFERENCE_HEADER**, or **SYSTEM_DEFINED**.
value	String	Specifies the value of the header. If **value_type** is set to **SYSTEM_DEFINED**, the value can be **CLIENT-PORT**, **CLIENT-IP**, **ELB-PROTOCOL**, **ELB-ID**, **ELB-PORT**, **ELB-EIP**, or **ELB-VIP**. The value can contain 1 to 128 characters. ASCII codes 32 through 127 printable characters, asterisk (*), and question mark (?) are also supported. The value cannot start or end with a space.

Table 5-529 RemoveHeadersConfig

Parameter	Type	Description
configs	Array of **RemoveHeaderConfig** objects	Specifies the headers you want to remove from the request that matches the forwarding rule.

Table 5-530 RemoveHeaderConfig

Parameter	Type	Description
key	String	Specifies the key of the header you want to remove from the request that matches the forwarding rule. The value is a string of 1 to 40 case-insensitive characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. The key cannot be the following: connection, upgrade, content-length, transfer-encoding, keep-alive, te, host, cookie, remoteip, authority, x-forwarded-host, x-forwarded-for, x-forwarded-for-port, x-forwarded-tls-certificate-id, x-forwarded-tls-protocol, x-forwarded-tls-cipher, x-forwarded-elb-ip, x-forwarded-port, x-forwarded-elb-id, x-forwarded-elb-vip, x-real-ip, x-forwarded-proto, x-nuwa-trace-ne-in, or x-nuwa-trace-ne-out.

Table 5-531 TrafficLimitConfig

Parameter	Type	Description
qps	Integer	Specifies the maximum number of queries per second (QPS). The value ranges from **0** to **100000**. **0** indicates that QPS is not limited.

Parameter	Type	Description
per_source_ip_qps	Integer	Specifies the maximum number of queries per second (QPS) from a source IP address. This parameter is not available for QUIC listeners. The value can be **0** or **null**. The value ranges from **0** to **100000**. **0** indicates that QPS is not limited. If **qps** is not set to **0**, **per_source_ip_qps** must be specified a smaller value than **qps**.
burst	Integer	Specifies the maximum number of queries per second (QPS) from a source IP address. The value ranges from **0** to **100000**. If the number of requests exceeds the value specified for **qps** but not reaches the value specified for **burst**, 503 status code will not be returned.

Example Requests

Creating a redirection for a listener.

```
POST https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/l7policies

{
  "l7policy" : {
    "action" : "REDIRECT_TO_LISTENER",
    "listener_id" : "e2220d2a-3faf-44f3-8cd6-0c42952bd0ab",
    "redirect_listener_id" : "48a97732-449e-4aab-b561-828d29e45050"
  }
}
```

Example Responses

Status code: 201

Normal response to POST requests.

```
{
  "request_id" : "b60d1d9a-5263-45b0-b1d6-2810ac7c52a1",
  "l7policy" : {
    "redirect_pool_id" : "768e9e8c-e7cb-4fef-b24b-af9399dbb240",
    "description" : "",
    "admin_state_up" : true,
    "rules" : [ {
      "id" : "c5c2d625-676b-431e-a4c7-c59cc2664881"
    } ],
    "project_id" : "7a9941d34fc1497d8d0797429ecfd354",
    "listener_id" : "cdb03a19-16b7-4e6b-bfec-047aeec74f56",
    "redirect_url" : null,
    "redirect_url_config" : null,
    "redirect_pools_config" : {
```



```
    "pool_id" : "722e9e8c-e7cb-4fef-b24b-af9399dbb240",
    "weight" : 12
  },
  "redirect_pools_sticky_session_config" : {
    "timeout" : 23,
    "enable" : false
  },
  "fixed_response_config" : null,
  "redirect_listener_id" : null,
  "action" : "REDIRECT_TO_POOL",
  "position" : 100,
  "priority" : null,
  "provisioning_status" : "ACTIVE",
  "id" : "01832d99-bbd8-4340-9d0c-6ff8f7a37307",
  "name" : "l7policy-67"
 }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Creating a redirection for a listener.

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class CreateL7PolicySolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateL7PolicyRequest request = new CreateL7PolicyRequest();
        CreateL7PolicyRequestBody body = new CreateL7PolicyRequestBody();
        CreateL7PolicyOption l7policybody = new CreateL7PolicyOption();
        l7policybody.withAction("REDIRECT_TO_LISTENER")
            .withListenerId("e2220d2a-3faf-44f3-8cd6-0c42952bd0ab")
            .withRedirectListenerId("48a97732-449e-4aab-b561-828d29e45050");
        body.withL7policy(l7policybody);
        request.withBody(body);
```



```
        try {
            CreateL7PolicyResponse response = client.createL7Policy(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

Creating a redirection for a listener.

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateL7PolicyRequest()
        l7policybody = CreateL7PolicyOption(
            action="REDIRECT_TO_LISTENER",
            listener_id="e2220d2a-3faf-44f3-8cd6-0c42952bd0ab",
            redirect_listener_id="48a97732-449e-4aab-b561-828d29e45050"
        )
        request.body = CreateL7PolicyRequestBody(
            l7policy=l7policybody
        )
        response = client.create_l7_policy(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

Creating a redirection for a listener.


```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateL7PolicyRequest{}
    redirectListenerIdL7policy:= "48a97732-449e-4aab-b561-828d29e45050"
    l7policybody := &model.CreateL7PolicyOption{
        Action: "REDIRECT_TO_LISTENER",
        ListenerId: "e2220d2a-3faf-44f3-8cd6-0c42952bd0ab",
        RedirectListenerId: &redirectListenerIdL7policy,
    }
    request.Body = &model.CreateL7PolicyRequestBody{
        L7policy: l7policybody,
    }
    response, err := client.CreateL7Policy(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 POST requests.

Error Codes

See **Error Codes**.

5.14.2 Querying Forwarding Policies

Function

This API is used to query all forwarding policies.

Constraints

This API has the following constraints:

- Parameters **marker**, **limit**, and **page_reverse** are used for pagination query.
- Parameters **marker** and **page_reverse** take effect only when they are used together with parameter **limit**.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/l7policies

Table 5-532 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Table 5-533 Query Parameters

Parameter	Mandatory	Type	Description
marker	No	String	Specifies the ID of the last record on the previous page. Note: • This parameter must be used together with **limit**. • If this parameter is not specified, the first page will be queried. • This parameter cannot be left blank or set to an invalid ID.

Parameter	Mandatory	Type	Description
limit	No	Integer	Specifies the number of records on each page. Value range: 0–2000 Default value: 2000
page_reverse	No	Boolean	Specifies whether to use reverse query. Value options: • **true**: Query the previous page. • **false** (default): Query the next page. Note: • This parameter must be used together with **limit**. • If **page_reverse** is set to **true** and you want to query the previous page, set the value of **marker** to the value of **previous_marker**.

Parameter	Mandatory	Type	Description
enterprise_project_id	No	Array of strings	Specifies the ID of the enterprise project. • If **enterprise_project_id** is not specified, resources in all enterprise projects are queried by default. Fine-grained authorization is performed. The **elb:l7policies:list** permission must be assigned to the user group. • If **enterprise_project_id** is specified, the value can be a specific enterprise project ID or **all_granted_eps**. If the value is a specific enterprise project ID, only resources in the enterprise project are queried. If the value is **all_granted_eps**, resources in the enterprise projects with the **elb:l7policies:list** permission are queried. Multiple values can be queried in the format of *enterprise_project_id=xxx&enterprise_project_id=xxx*.
id	No	Array of strings	Specifies the forwarding policy ID. Multiple IDs can be queried in the format of *id=xxx&id=xxx*.
name	No	Array of strings	Specifies the forwarding policy name. Multiple names can be queried in the format of *name=xxx&name=xxx*.
description	No	Array of strings	Provides supplementary information about the forwarding policy. Multiple descriptions can be queried in the format of *description=xxx&description=xxx*.

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Specifies the administrative status of the forwarding policy. This parameter is unsupported. Please do not use it.
listener_id	No	Array of strings	Specifies the ID of the listener to which the forwarding policy is added. Multiple IDs can be queried in the format of *listener_id=xxx&listener_id=xxx*.
position	No	Array of integers	Specifies the forwarding policy priority. Multiple priorities can be queried in the format of *position=xxx&position=xxx*. This parameter is unsupported. Please do not use it.
action	No	Array of strings	Specifies where requests are forwarded. Value options: • **REDIRECT_TO_POOL**: Requests are forwarded to another backend server group. • **REDIRECT_TO_LISTENER**: Requests are redirected to an HTTPS listener. • **REDIRECT_TO_URL**: Requests are redirected to another URL. • **FIXED_RESPONSE**: A fixed response body is returned. Multiple values can be queried in the format of *action=xxx&action=xxx*.

Parameter	Mandatory	Type	Description
redirect_url	No	Array of strings	Specifies the URL to which requests will be forwarded. Multiple URLs can be queried in the format of *redirect_url=xxx&redirect_url=xxx*. This parameter is unsupported. Please do not use it.
redirect_pool_id	No	Array of strings	Specifies the ID of the backend server group to which requests will be forwarded. Multiple IDs can be queried in the format of *redirect_pool_id=xxx&redirect_pool_id=xxx*.
redirect_listener_id	No	Array of strings	Specifies the ID of the listener to which requests are redirected. Multiple IDs can be queried in the format of *redirect_listener_id=xxx&redirect_listener_id=xxx*.
provisioning_status	No	Array of strings	Specifies the provisioning status of the forwarding policy. • **ACTIVE**: The forwarding policy is provisioned successfully. • **ERROR**: The forwarding policy has the same rule as another forwarding policy added to the same listener. Multiple provisioning statuses can be queried in the format of *provisioning_status=xxx&provisioning_status=xxx*.

Parameter	Mandatory	Type	Description
display_all_rules	No	Boolean	Specifies whether to display details about the forwarding rule in the forwarding policy. Value options: • **true**: Details about the forwarding rule are displayed. • **false**: Only the rule ID is displayed.
priority	No	Array of integers	Specifies the forwarding policy priority. A smaller value indicates a higher priority. Multiple priorities can be queried in the format of *position=xxx&position=xxx*.

Request Parameters

Table 5-534 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-535 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
page_info	**PageInfo** object	Shows pagination information.
l7policies	Array of **L7Policy** objects	Lists the forwarding policies.

Table 5-536 PageInfo

Parameter	Type	Description
previous_marker	String	Specifies the ID of the first record in the pagination query result. When **page_reverse** is set to **true**, this parameter is used together to query resources on the previous page.
next_marker	String	Specifies the ID of the last record in the pagination query result.
current_count	Integer	Specifies the number of records.

Table 5-537 L7Policy

Parameter	Type	Description
action	String	Specifies where requests will be forwarded. Value options: • **REDIRECT_TO_POOL**: Requests will be forwarded to another backend server group. • **REDIRECT_TO_LISTENER**: Requests will be redirected to an HTTPS listener. • **REDIRECT_TO_URL**: Requests will be redirected to another URL. • **FIXED_RESPONSE**: A fixed response body will be returned. Note: • **REDIRECT_TO_LISTENER** has the highest priority. If requests are to be redirected to an HTTPS listener, other forwarding policies of the listener will become invalid. • If **action** is set to **REDIRECT_TO_POOL**, the listener's protocol must be HTTP, HTTPS, or TERMINATED_HTTPS. • If **action** is set to **REDIRECT_TO_LISTENER**, the listener's protocol must be HTTP.
admin_state_up	Boolean	Specifies the administrative status of the forwarding policy. Note: The value can only be **true**.

Parameter	Type	Description
description	String	Provides supplementary information about the forwarding policy.
id	String	Specifies the forwarding policy ID.
listener_id	String	Specifies the ID of the listener to which the forwarding policy is added.
name	String	Specifies the forwarding policy name.
position	Integer	Specifies the forwarding policy priority. This parameter cannot be updated. This parameter is unsupported. Please do not use it.

Parameter	Type	Description
priority	Integer	Specifies the forwarding policy priority. A smaller value indicates a higher priority. Value ranges: • If **action** is set to **REDIRECT_TO_LISTENER**, the priority ranges from 0 to 10,000. • If **action** is set to other values, the priority ranges from 1 to 10,000. Default value options: • If this parameter is not passed and **enhance_l7policy_enable** is set to **false**, the priority of the new forwarding policy is **1**. • If **action** is set to **REDIRECT_TO_LISTENER**, the priority of the new forwarding policy is **0**. • If **action** is set to other values, the priority of the new forwarding policy will be a sum of 1 and the highest priority of existing forwarding policy in the same listener by default. – If no forwarding policies exist, the priority of the new forwarding policy will be **1** by default. – If the highest priority of existing forwarding policies is the maximum value (10,000), the forwarding policy will fail to be created because the final priority for creating the forwarding policy is the sum of 1 and 10,000, which exceeds the maximum value. In this case, specify a value or adjust the priorities of existing forwarding policies. Note: • The value must be unique for forwarding policies of the same listener. • This parameter takes effect only when **enhance_l7policy_enable** is

Parameter	Type	Description
		set to **true**. If this parameter is passed and **enhance_l7policy_enable** is set to **false**, an error will be returned. • If **enhance_l7policy_enable** is not enabled, forwarding policies are automatically prioritized based on the original policy sorting logic. The priorities of domain names are independent from each other. For the same domain name, the priorities are sorted in the order of exact match (**EQUAL_TO**), prefix match (**STARTS_WITH**), and regular expression match (**REGEX**). If the matching types are the same, the longer the path is, the higher the priority is. If a forwarding policy contains only a domain name without a path specified, the path is **/**, and prefix match is used by default. This parameter is supported by forwarding policies of shared load balancers.
project_id	String	Specifies the project ID of the forwarding policy.
provisioning_status	String	Specifies the provisioning status of the forwarding policy. The value can be **ACTIVE** or **ERROR**. • **ACTIVE** (default): The forwarding policy is provisioned successfully. • **ERROR**: Another forwarding policy of the same listener has the same forwarding rule.
redirect_pool_id	String	Specifies the ID of the backend server group to which the requests are forwarded. Note: This parameter is valid only when **action** is set to **REDIRECT_TO_POOL**.

Parameter	Type	Description
redirect_listener_id	String	Specifies the ID of the listener to which requests are redirected. Note: • This parameter is mandatory when **action** is set to **REDIRECT_TO_LISTENER**. • The listener's protocol must be **HTTPS** or **TERMINATED_HTTPS**. • A listener added to another load balancer is not allowed. • This parameter cannot be passed in the API for adding or updating a forwarding policy if **action** is set to **REDIRECT_TO_POOL**.
redirect_url	String	Specifies the URL to which requests are forwarded. Format: *protocol://host:port/path?query* This parameter is unsupported. Please do not use it.
rules	Array of **RuleRef** objects	Lists the forwarding rules in the forwarding policy.

Parameter	Type	Description
redirect_url_config	**RedirectUrlConfig** object	Specifies the URL to which requests are forwarded. Note: • This parameter will take effect only when advanced forwarding is enabled (**enhance_l7policy_enable** is set to **true**). If it is passed when **enhance_l7policy_enable** is set to **false**, an error will be returned. • This parameter is mandatory when **action** is set to **REDIRECT_TO_URL**. It cannot be specified if the value of **action** is not **REDIRECT_TO_URL**. • For shared load balancers, this parameter is unsupported. If it is passed, an error will be returned. • At least one of the four parameters (**protocol**, **host**, **port**, and **path**) must be passed, or their values cannot be set to **${xxx}** at the same time. **${xxx}** indicates that the value in the request will be used. For example, **${host}** indicates the host in the URL to be redirected. • The values of **protocol** and **port** cannot be the same as those of the associated listener, and either **host** or **path** must be passed or their values cannot be **${xxx}** at the same time. Value format: *protocol://host:port/path?query*
redirect_pools_config	Array of **RedirectPoolsConfig** objects	Specifies the backend server groups that the requests are forwarded to. Note: A maximum of 5 backend server groups can be configured for a forwarding policy.

Parameter	Type	Description
redirect_pools_sticky_session_config	**RedirectPoolsStickySessionConfig** object	Specifies whether to enable sticky session for backend server groups configured for a forwarding policy. The load balancer generates a cookie after it receives a request from a client. All subsequent requests with the same cookie are routed to the same backend server groups. This parameter is unsupported for shared load balancers. If it is passed, an error will be returned.
redirect_pools_extend_config	**RedirectPoolsExtendConfig** object	Specifies the backend server group that requests are forwarded to. Note: This parameter takes effect only when **action** is set to **REDIRECT_TO_POOL**.
fixed_response_config	**FixtedResponseConfig** object	Specifies the configuration of the page that will be returned. Note: • This parameter will take effect when **enhance_l7policy_enable** is set to **true**. If this parameter is passed and **enhance_l7policy_enable** is set to **false**, an error will be returned. • This parameter is mandatory when **action** is set to **FIXED_RESPONSE**. It cannot be specified if the value of **action** is not **FIXED_RESPONSE**. • For shared load balancers, this parameter is unsupported. If it is passed, an error will be returned.
created_at	String	Specifies the time when the forwarding policy was added. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.

Parameter	Type	Description
updated_at	String	Specifies the time when the forwarding policy was updated. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
enterprise_project_id	String	Specifies the ID of the enterprise project.

Table 5-538 RuleRef

Parameter	Type	Description
id	String	Specifies the forwarding rule ID.

Table 5-539 RedirectUrlConfig

Parameter	Type	Description
protocol	String	Specifies the protocol for redirection. The value can be **HTTP**, **HTTPS**, or **${protocol}**. **${protocol}** indicates that the protocol of the request will be used.
host	String	Specifies the name of the host that requests are redirected to. The value can contain only letters, digits, hyphens (-), and periods (.) and must start with a letter or digit. The default value is **${host}**, indicating that the host of the request will be used.
port	String	Specifies the port that requests are redirected to. The default value is **${port}**, indicating that the port of the request will be used.

Parameter	Type	Description
path	String	Specifies the path that requests are redirected to. The value can contain only letters, digits, and special characters: _~';@^-%#&$.*+?,=!:|\/()[]{} and must start with a slash (/). $1, $2, $3, and all the way to $9 match the wildcard asterisk (*) in the request URL. The default value is **${path}**, indicating that the path of the request will be used.
query	String	Specifies the query string set in the URL for redirection. The value is case-sensitive and can contain only letters, digits, and special characters: !$&'()*+,-./:;=?@^_`. $1, $2, $3, and all the way to $9 match the wildcard asterisk (*) in the request URL. The default value is **${query}**, indicating that the query string of the request will be used. For example, in the URL **https://www.example.com:8080/elb?type=loadbalancer**, **${query}** indicates **type=loadbalancer**. If this parameter is set to **${query}&name=my_name**, the URL will be redirected to **https://www.example.com:8080/elb?type=loadbalancer&name=my_name**.
status_code	String	Specifies the status code returned after the requests are redirected. The value can be **301**, **302**, **303**, **307**, or **308**.
insert_headers_config	**InsertHeadersConfig** object	Specifies the headers you want to write into the request that matches the forwarding rule.
remove_headers_config	**RemoveHeadersConfig** object	Specifies the headers you want to remove from the request that matches the forwarding rule.

Table 5-540 RedirectPoolsConfig

Parameter	Type	Description
pool_id	String	Specifies the ID of the backend server group.
weight	Integer	Specifies the weight of the backend server group. The value ranges from **0** to **100**. Requests are routed to backend server groups based on their weights. Backend server groups with higher weights receive proportionately more requests. No requests will be routed to a backend server group with a weight of 0.

Table 5-541 RedirectPoolsStickySessionConfig

Parameter	Type	Description
enable	Boolean	Specifies whether to enable sticky session for backend server groups configured in a forwarding policy. The default value is **false**, indicating that sticky session is disabled.
timeout	Integer	Specifies the duration that a session persists. The value ranges from **1** to **1440** (default), in minutes.

Table 5-542 RedirectPoolsExtendConfig

Parameter	Type	Description
rewrite_url_enable	Boolean	Specifies whether to set **rewrite_url_enable** to **true**.
rewrite_url_config	**RewriteUrlConfig** object	Specifies the URL for the backend server group that requests are forwarded to. This parameter takes effect only when **action** is set to **REDIRECT_TO_POOL**.
insert_headers_config	**InsertHeadersConfig** object	Specifies the headers you want to write into the request that matches the forwarding rule.

Parameter	Type	Description
remove_headers_config	**RemoveHeadersConfig** object	Specifies the headers you want to remove from the request that matches the forwarding rule.
traffic_limit_config	**TrafficLimitConfig** object	Specifies how requests are limited.
cors_config	**CorsConfig** object	Specifies the CORS configurations.

Table 5-543 RewriteUrlConfig

Parameter	Type	Description
host	String	Specifies the domain name of the host that requests are redirected to. The domain name can contain only letters, digits, hyphens (-), and periods (.), and must start with a letter or digit. The default value is **${host}**, indicating that the host of the request will be used.
path	String	Specifies the path that requests are redirected to. The default value is **${path}**, indicating that the path of the request will be used. The value can contain only letters, digits, and special characters: _~';@^-%#&$.+?,=!:|/() and must start with a slash (/). $1, $2, $3, and all the way to $9 match the wildcard asterisk (*) in the request URL. If the number of regular expression match groups is less than the specified number, **${path}** is empty. If the dollar sign ($) is followed by a letter, the matching result is empty until the next special character appears, for example, **$abc#123**, and the matching result is **#123**. If the dollar sign ($) is followed by a special character, for example, **$#**, the matching result is **$#**.

Parameter	Type	Description
query	String	Specifies the query string set in the URL for redirection. The value is case-sensitive and can contain only letters, digits, and special characters: !$&'()*+,-./:;=?@^_`. *$1, $2, $3, and all the way to $9 match the wildcard asterisk (*)* in the request URL. The default value is **${query}**, indicating that the query string of the request will be used. If the number of regular expression match groups is less than the specified number, **${path}** is empty. If the dollar sign ($) is followed by a letter, the matching result is empty until the next special character appears, for example, **$abc#123**, and the matching result is **#123**. If the dollar sign ($) is followed by a special character, for example, **$#**, the matching result is **$#**.

Table 5-544 CorsConfig

Parameter	Type	Description
allow_origin	Array of strings	Specifies the origins that are allowed to access cross-origin resources through a browser. The origin can be a wildcard (*) or one or more URLs. Constraints: • Each URL must start with **http://** or **https://**, followed by a valid domain name or level-1 wildcard domain name, for example, http://*.test.abc.example.com. • It is optional to include a port number (ranging from 1 to 65535) in the URL.
allow_methods	Array of strings	Specifies the HTTP methods that the specified URLs can use to access cross-origin resources.
allow_headers	Array of strings	Specifies the request headers that can be carried in CORS requests.
expose_headers	Array of strings	Specifies the headers that can be exposed.

Parameter	Type	Description
allow_credentials	Boolean	Specifies whether to allow credentials in CORS requests. Value options: • **true**: Credentials are allowed. • **false**: Credentials are not allowed.
max_age	Long	Specifies the maximum duration a preflight request can be cached, in seconds. Value range: -1 to 172800

Table 5-545 FixtedResponseConfig

Parameter	Type	Description
status_code	String	Specifies the HTTP status code configured in the forwarding policy. The value can be any integer in the range of 200–299, 400–499, or 500–599.
content_type	String	Specifies the format of the response body. The value can be **text/plain**, **text/css**, **text/html**, **application/javascript**, or **application/json**.
message_body	String	Specifies the content of the response message body.
insert_headers_config	**InsertHeadersConfig** object	Specifies the headers you want to write into the request that matches the forwarding rule.
remove_headers_config	**RemoveHeadersConfig** object	Specifies the headers you want to remove from the request that matches the forwarding rule.
traffic_limit_config	**TrafficLimitConfig** object	Specifies how requests are limited.

Table 5-546 InsertHeadersConfig

Parameter	Type	Description
configs	Array of **InsertHeaderConfig** objects	Specifies the headers you want to write into the request that matches the forwarding rule.

Table 5-547 InsertHeaderConfig

Parameter	Type	Description
key	String	Specifies the key of the header you want to write into the request that matches the forwarding rule. The value is a string of 1 to 40 case-insensitive characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. The key cannot be the following: connection, upgrade, content-length, transfer-encoding, keep-alive, te, host, cookie, remoteip, authority, x-forwarded-host, x-forwarded-for, x-forwarded-for-port, x-forwarded-tls-certificate-id, x-forwarded-tls-protocol, x-forwarded-tls-cipher, x-forwarded-elb-ip, x-forwarded-port, x-forwarded-elb-id, x-forwarded-elb-vip, x-real-ip, x-forwarded-proto, x-nuwa-trace-ne-in, or x-nuwa-trace-ne-out.
value_type	String	Specifies the value type of the header. The value can be **USER_DEFINED**, **REFERENCE_HEADER**, or **SYSTEM_DEFINED**.
value	String	Specifies the value of the header. If **value_type** is set to **SYSTEM_DEFINED**, the value can be **CLIENT-PORT**, **CLIENT-IP**, **ELB-PROTOCOL**, **ELB-ID**, **ELB-PORT**, **ELB-EIP**, or **ELB-VIP**. The value can contain 1 to 128 characters. ASCII codes 32 through 127 printable characters, asterisk (*), and question mark (?) are also supported. The value cannot start or end with a space.

Table 5-548 RemoveHeadersConfig

Parameter	Type	Description
configs	Array of **RemoveHeaderConfig** objects	Specifies the headers you want to remove from the request that matches the forwarding rule.

Table 5-549 RemoveHeaderConfig

Parameter	Type	Description
key	String	Specifies the key of the header you want to remove from the request that matches the forwarding rule. The value is a string of 1 to 40 case-insensitive characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. The key cannot be the following: connection, upgrade, content-length, transfer-encoding, keep-alive, te, host, cookie, remoteip, authority, x-forwarded-host, x-forwarded-for, x-forwarded-for-port, x-forwarded-tls-certificate-id, x-forwarded-tls-protocol, x-forwarded-tls-cipher, x-forwarded-elb-ip, x-forwarded-port, x-forwarded-elb-id, x-forwarded-elb-vip, x-real-ip, x-forwarded-proto, x-nuwa-trace-ne-in, or x-nuwa-trace-ne-out.

Table 5-550 TrafficLimitConfig

Parameter	Type	Description
qps	Integer	Specifies the maximum number of queries per second (QPS). The value ranges from **0** to **100000**. **0** indicates that QPS is not limited.

Parameter	Type	Description
per_source_ip_qps	Integer	Specifies the maximum number of queries per second (QPS) from a source IP address. This parameter is not available for QUIC listeners. The value can be **0** or **null**. The value ranges from **0** to **100000**. **0** indicates that QPS is not limited. If **qps** is not set to **0**, **per_source_ip_qps** must be specified a smaller value than **qps**.
burst	Integer	Specifies the maximum number of queries per second (QPS) from a source IP address. The value ranges from **0** to **100000**. If the number of requests exceeds the value specified for **qps** but not reaches the value specified for **burst**, 503 status code will not be returned.

Example Requests

Querying forwarding policies

```
GET https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/l7policies?display_all_rules=true
```

Example Responses

Status code: 200

Successful request.


```
{
  "request_id" : "d3c67339-be91-4813-bb24-85728a5d326a",
  "l7policies" : [ {
    "redirect_pool_id" : "768e9e8c-e7cb-4fef-b24b-af9399dbb240",
    "description" : "",
    "admin_state_up" : true,
    "rules" : [ {
      "id" : "c5c2d625-676b-431e-a4c7-c59cc2664881"
    } ],
    "project_id" : "7a9941d34fc1497d8d0797429ecfd354",
    "listener_id" : "cdb03a19-16b7-4e6b-bfec-047aeec74f56",
    "redirect_url" : null,
    "redirect_url_config" : null,
    "redirect_pools_config" : {
      "pool_id" : "722e9e8c-e7cb-4fef-b24b-af9399dbb240",
      "weight" : 12
    },
    "redirect_pools_sticky_session_config" : {
      "timeout" : 23,
      "enable" : false
    },
    "fixed_response_config" : null,
```



```
    "redirect_listener_id" : null,
    "action" : "REDIRECT_TO_POOL",
    "position" : 100,
    "priority" : null,
    "provisioning_status" : "ACTIVE",
    "id" : "01832d99-bbd8-4340-9d0c-6ff8f7a37307",
    "name" : "l7policy-67"
  }, {
    "redirect_pool_id" : null,
    "description" : "",
    "admin_state_up" : true,
    "rules" : [ {
      "id" : "390f3a9f-670d-4ca6-b72c-6be8a48a8a00"
    } ],
    "project_id" : "7a9941d34fc1497d8d0797429ecfd354",
    "listener_id" : "bd782cbf-fb5e-411a-9295-530bdec05058",
    "redirect_url" : null,
    "redirect_url_config" : null,
    "redirect_pools_config" : {
      "pool_id" : "722e9e8c-e7cb-4fef-b24b-af9399dbb240",
      "weight" : 12
    },
    "redirect_pools_sticky_session_config" : {
      "timeout" : 23,
      "enable" : false
    },
    "fixed_response_config" : {
      "content_type" : "text/plain",
      "message_body" : "",
      "status_code" : "207"
    },
    "redirect_listener_id" : null,
    "action" : "FIXED_RESPONSE",
    "position" : 6,
    "priority" : 2,
    "provisioning_status" : "ACTIVE",
    "id" : "049a8635-9754-444e-94aa-678993b39cd6",
    "name" : "l7policy-67"
  } ],
  "page_info" : {
    "next_marker" : "2587d8b1-9e8d-459c-9081-7bccaa075d2b",
    "previous_marker" : "01832d99-bbd8-4340-9d0c-6ff8f7a37307",
    "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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ListL7PoliciesSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ListL7PoliciesRequest request = new ListL7PoliciesRequest();
        try {
            ListL7PoliciesResponse response = client.listL7Policies(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListL7PoliciesRequest()
        response = client.list_l7_policies(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListL7PoliciesRequest{}
    response, err := client.ListL7Policies(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	Successful request.

Error Codes

See **Error Codes**.

5.14.3 Querying the Details of a Forwarding Policy

Function

This API is used to view the details of a forwarding policy.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/l7policies/{l7policy_id}

Table 5-551 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
l7policy_id	Yes	String	Specifies the forwarding policy ID.

Request Parameters

Table 5-552 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-553 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
l7policy	**L7Policy** object	Specifies the forwarding policy.

Table 5-554 L7Policy

Parameter	Type	Description
action	String	Specifies where requests will be forwarded. Value options: • **REDIRECT_TO_POOL**: Requests will be forwarded to another backend server group. • **REDIRECT_TO_LISTENER**: Requests will be redirected to an HTTPS listener. • **REDIRECT_TO_URL**: Requests will be redirected to another URL. • **FIXED_RESPONSE**: A fixed response body will be returned. Note: • **REDIRECT_TO_LISTENER** has the highest priority. If requests are to be redirected to an HTTPS listener, other forwarding policies of the listener will become invalid. • If **action** is set to **REDIRECT_TO_POOL**, the listener's protocol must be HTTP, HTTPS, or TERMINATED_HTTPS. • If **action** is set to **REDIRECT_TO_LISTENER**, the listener's protocol must be HTTP.
admin_state_up	Boolean	Specifies the administrative status of the forwarding policy. Note: The value can only be **true**.
description	String	Provides supplementary information about the forwarding policy.
id	String	Specifies the forwarding policy ID.
listener_id	String	Specifies the ID of the listener to which the forwarding policy is added.
name	String	Specifies the forwarding policy name.
position	Integer	Specifies the forwarding policy priority. This parameter cannot be updated. This parameter is unsupported. Please do not use it.

Parameter	Type	Description
priority	Integer	Specifies the forwarding policy priority. A smaller value indicates a higher priority. Value ranges: • If **action** is set to **REDIRECT_TO_LISTENER**, the priority ranges from 0 to 10,000. • If **action** is set to other values, the priority ranges from 1 to 10,000. Default value options: • If this parameter is not passed and **enhance_l7policy_enable** is set to **false**, the priority of the new forwarding policy is **1**. • If **action** is set to **REDIRECT_TO_LISTENER**, the priority of the new forwarding policy is **0**. • If **action** is set to other values, the priority of the new forwarding policy will be a sum of 1 and the highest priority of existing forwarding policy in the same listener by default. – If no forwarding policies exist, the priority of the new forwarding policy will be **1** by default. – If the highest priority of existing forwarding policies is the maximum value (10,000), the forwarding policy will fail to be created because the final priority for creating the forwarding policy is the sum of 1 and 10,000, which exceeds the maximum value. In this case, specify a value or adjust the priorities of existing forwarding policies. Note: • The value must be unique for forwarding policies of the same listener. • This parameter takes effect only when **enhance_l7policy_enable** is

Parameter	Type	Description
		set to **true**. If this parameter is passed and **enhance_l7policy_enable** is set to **false**, an error will be returned. • If **enhance_l7policy_enable** is not enabled, forwarding policies are automatically prioritized based on the original policy sorting logic. The priorities of domain names are independent from each other. For the same domain name, the priorities are sorted in the order of exact match (**EQUAL_TO**), prefix match (**STARTS_WITH**), and regular expression match (**REGEX**). If the matching types are the same, the longer the path is, the higher the priority is. If a forwarding policy contains only a domain name without a path specified, the path is **/**, and prefix match is used by default. This parameter is supported by forwarding policies of shared load balancers.
project_id	String	Specifies the project ID of the forwarding policy.
provisioning_status	String	Specifies the provisioning status of the forwarding policy. The value can be **ACTIVE** or **ERROR**. • **ACTIVE** (default): The forwarding policy is provisioned successfully. • **ERROR**: Another forwarding policy of the same listener has the same forwarding rule.
redirect_pool_id	String	Specifies the ID of the backend server group to which the requests are forwarded. Note: This parameter is valid only when **action** is set to **REDIRECT_TO_POOL**.

Parameter	Type	Description
redirect_listener_id	String	Specifies the ID of the listener to which requests are redirected. Note: • This parameter is mandatory when **action** is set to **REDIRECT_TO_LISTENER**. • The listener's protocol must be **HTTPS** or **TERMINATED_HTTPS**. • A listener added to another load balancer is not allowed. • This parameter cannot be passed in the API for adding or updating a forwarding policy if **action** is set to **REDIRECT_TO_POOL**.
redirect_url	String	Specifies the URL to which requests are forwarded. Format: *protocol://host:port/path?query* This parameter is unsupported. Please do not use it.
rules	Array of **RuleRef** objects	Lists the forwarding rules in the forwarding policy.

Parameter	Type	Description
redirect_url_config	**RedirectUrlConfig** object	Specifies the URL to which requests are forwarded. Note: • This parameter will take effect only when advanced forwarding is enabled (**enhance_l7policy_enable** is set to **true**). If it is passed when **enhance_l7policy_enable** is set to **false**, an error will be returned. • This parameter is mandatory when **action** is set to **REDIRECT_TO_URL**. It cannot be specified if the value of **action** is not **REDIRECT_TO_URL**. • For shared load balancers, this parameter is unsupported. If it is passed, an error will be returned. • At least one of the four parameters (**protocol**, **host**, **port**, and **path**) must be passed, or their values cannot be set to **${xxx}** at the same time. **${xxx}** indicates that the value in the request will be used. For example, **${host}** indicates the host in the URL to be redirected. • The values of **protocol** and **port** cannot be the same as those of the associated listener, and either **host** or **path** must be passed or their values cannot be **${xxx}** at the same time. Value format: *protocol://host:port/path?query*
redirect_pools_config	Array of **RedirectPoolsConfig** objects	Specifies the backend server groups that the requests are forwarded to. Note: A maximum of 5 backend server groups can be configured for a forwarding policy.

Parameter	Type	Description
redirect_pools_sticky_session_config	**RedirectPoolsStickySessionConfig** object	Specifies whether to enable sticky session for backend server groups configured for a forwarding policy. The load balancer generates a cookie after it receives a request from a client. All subsequent requests with the same cookie are routed to the same backend server groups. This parameter is unsupported for shared load balancers. If it is passed, an error will be returned.
redirect_pools_extend_config	**RedirectPoolsExtendConfig** object	Specifies the backend server group that requests are forwarded to. Note: This parameter takes effect only when **action** is set to **REDIRECT_TO_POOL**.
fixed_response_config	**FixtedResponseConfig** object	Specifies the configuration of the page that will be returned. Note: • This parameter will take effect when **enhance_l7policy_enable** is set to **true**. If this parameter is passed and **enhance_l7policy_enable** is set to **false**, an error will be returned. • This parameter is mandatory when **action** is set to **FIXED_RESPONSE**. It cannot be specified if the value of **action** is not **FIXED_RESPONSE**. • For shared load balancers, this parameter is unsupported. If it is passed, an error will be returned.
created_at	String	Specifies the time when the forwarding policy was added. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.

Parameter	Type	Description
updated_at	String	Specifies the time when the forwarding policy was updated. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
enterprise_project_id	String	Specifies the ID of the enterprise project.

Table 5-555 RuleRef

Parameter	Type	Description
id	String	Specifies the forwarding rule ID.

Table 5-556 RedirectUrlConfig

Parameter	Type	Description
protocol	String	Specifies the protocol for redirection. The value can be **HTTP**, **HTTPS**, or **${protocol}**. **${protocol}** indicates that the protocol of the request will be used.
host	String	Specifies the name of the host that requests are redirected to. The value can contain only letters, digits, hyphens (-), and periods (.) and must start with a letter or digit. The default value is **${host}**, indicating that the host of the request will be used.
port	String	Specifies the port that requests are redirected to. The default value is **${port}**, indicating that the port of the request will be used.

Parameter	Type	Description
path	String	Specifies the path that requests are redirected to. The value can contain only letters, digits, and special characters: _~';@^-%#&$.*+?,=!:|\/()[]{} and must start with a slash (/). $1, $2, $3, and all the way to $9 match the wildcard asterisk (*) in the request URL. The default value is **${path}**, indicating that the path of the request will be used.
query	String	Specifies the query string set in the URL for redirection. The value is case-sensitive and can contain only letters, digits, and special characters: !$&'()*+,-./:;=?@^_`. $1, $2, $3, and all the way to $9 match the wildcard asterisk (*) in the request URL. The default value is **${query}**, indicating that the query string of the request will be used. For example, in the URL **https://www.example.com:8080/elb?type=loadbalancer**, **${query}** indicates **type=loadbalancer**. If this parameter is set to **${query}&name=my_name**, the URL will be redirected to **https://www.example.com:8080/elb?type=loadbalancer&name=my_name**.
status_code	String	Specifies the status code returned after the requests are redirected. The value can be **301**, **302**, **303**, **307**, or **308**.
insert_headers_config	**InsertHeadersConfig** object	Specifies the headers you want to write into the request that matches the forwarding rule.
remove_headers_config	**RemoveHeadersConfig** object	Specifies the headers you want to remove from the request that matches the forwarding rule.

Table 5-557 RedirectPoolsConfig

Parameter	Type	Description
pool_id	String	Specifies the ID of the backend server group.
weight	Integer	Specifies the weight of the backend server group. The value ranges from **0** to **100**. Requests are routed to backend server groups based on their weights. Backend server groups with higher weights receive proportionately more requests. No requests will be routed to a backend server group with a weight of 0.

Table 5-558 RedirectPoolsStickySessionConfig

Parameter	Type	Description
enable	Boolean	Specifies whether to enable sticky session for backend server groups configured in a forwarding policy. The default value is **false**, indicating that sticky session is disabled.
timeout	Integer	Specifies the duration that a session persists. The value ranges from **1** to **1440** (default), in minutes.

Table 5-559 RedirectPoolsExtendConfig

Parameter	Type	Description
rewrite_url_enable	Boolean	Specifies whether to set **rewrite_url_enable** to **true**.
rewrite_url_config	**RewriteUrlConfig** object	Specifies the URL for the backend server group that requests are forwarded to. This parameter takes effect only when **action** is set to **REDIRECT_TO_POOL**.
insert_headers_config	**InsertHeadersConfig** object	Specifies the headers you want to write into the request that matches the forwarding rule.

Parameter	Type	Description
remove_headers_config	**RemoveHeadersConfig** object	Specifies the headers you want to remove from the request that matches the forwarding rule.
traffic_limit_config	**TrafficLimitConfig** object	Specifies how requests are limited.
cors_config	**CorsConfig** object	Specifies the CORS configurations.

Table 5-560 RewriteUrlConfig

Parameter	Type	Description
host	String	Specifies the domain name of the host that requests are redirected to. The domain name can contain only letters, digits, hyphens (-), and periods (.), and must start with a letter or digit. The default value is **${host}**, indicating that the host of the request will be used.
path	String	Specifies the path that requests are redirected to. The default value is **${path}**, indicating that the path of the request will be used. The value can contain only letters, digits, and special characters: _~';@^-%#&$.+?,=!:|/() and must start with a slash (/). $1, $2, $3, and all the way to $9 match the wildcard asterisk (*) in the request URL. If the number of regular expression match groups is less than the specified number, **${path}** is empty. If the dollar sign ($) is followed by a letter, the matching result is empty until the next special character appears, for example, **$abc#123**, and the matching result is **#123**. If the dollar sign ($) is followed by a special character, for example, **$#**, the matching result is **$#**.

Parameter	Type	Description
query	String	Specifies the query string set in the URL for redirection. The value is case-sensitive and can contain only letters, digits, and special characters: !$&'()*+,-./:;=?@^_`. *$1, $2, $3, and all the way to $9 match the wildcard asterisk ()* in the request URL. The default value is **${query}**, indicating that the query string of the request will be used. If the number of regular expression match groups is less than the specified number, **${path}** is empty. If the dollar sign ($) is followed by a letter, the matching result is empty until the next special character appears, for example, **$abc#123**, and the matching result is **#123**. If the dollar sign ($) is followed by a special character, for example, **$#**, the matching result is **$#**.

Table 5-561 CorsConfig

Parameter	Type	Description
allow_origin	Array of strings	Specifies the origins that are allowed to access cross-origin resources through a browser. The origin can be a wildcard (*) or one or more URLs. Constraints: • Each URL must start with **http://** or **https://**, followed by a valid domain name or level-1 wildcard domain name, for example, http://*.test.abc.example.com. • It is optional to include a port number (ranging from 1 to 65535) in the URL.
allow_methods	Array of strings	Specifies the HTTP methods that the specified URLs can use to access cross-origin resources.
allow_headers	Array of strings	Specifies the request headers that can be carried in CORS requests.
expose_headers	Array of strings	Specifies the headers that can be exposed.

Parameter	Type	Description
allow_credentials	Boolean	Specifies whether to allow credentials in CORS requests. Value options: • **true**: Credentials are allowed. • **false**: Credentials are not allowed.
max_age	Long	Specifies the maximum duration a preflight request can be cached, in seconds. Value range: -1 to 172800

Table 5-562 FixtedResponseConfig

Parameter	Type	Description
status_code	String	Specifies the HTTP status code configured in the forwarding policy. The value can be any integer in the range of 200–299, 400–499, or 500–599.
content_type	String	Specifies the format of the response body. The value can be **text/plain**, **text/css**, **text/html**, **application/javascript**, or **application/json**.
message_body	String	Specifies the content of the response message body.
insert_headers_config	**InsertHeadersConfig** object	Specifies the headers you want to write into the request that matches the forwarding rule.
remove_headers_config	**RemoveHeadersConfig** object	Specifies the headers you want to remove from the request that matches the forwarding rule.
traffic_limit_config	**TrafficLimitConfig** object	Specifies how requests are limited.

Table 5-563 InsertHeadersConfig

Parameter	Type	Description
configs	Array of **InsertHeaderConfig** objects	Specifies the headers you want to write into the request that matches the forwarding rule.

Table 5-564 InsertHeaderConfig

Parameter	Type	Description
key	String	Specifies the key of the header you want to write into the request that matches the forwarding rule. The value is a string of 1 to 40 case-insensitive characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. The key cannot be the following: connection, upgrade, content-length, transfer-encoding, keep-alive, te, host, cookie, remoteip, authority, x-forwarded-host, x-forwarded-for, x-forwarded-for-port, x-forwarded-tls-certificate-id, x-forwarded-tls-protocol, x-forwarded-tls-cipher, x-forwarded-elb-ip, x-forwarded-port, x-forwarded-elb-id, x-forwarded-elb-vip, x-real-ip, x-forwarded-proto, x-nuwa-trace-ne-in, or x-nuwa-trace-ne-out.
value_type	String	Specifies the value type of the header. The value can be **USER_DEFINED**, **REFERENCE_HEADER**, or **SYSTEM_DEFINED**.
value	String	Specifies the value of the header. If **value_type** is set to **SYSTEM_DEFINED**, the value can be **CLIENT-PORT**, **CLIENT-IP**, **ELB-PROTOCOL**, **ELB-ID**, **ELB-PORT**, **ELB-EIP**, or **ELB-VIP**. The value can contain 1 to 128 characters. ASCII codes 32 through 127 printable characters, asterisk (*), and question mark (?) are also supported. The value cannot start or end with a space.

Table 5-565 RemoveHeadersConfig

Parameter	Type	Description
configs	Array of **RemoveHeaderConfig** objects	Specifies the headers you want to remove from the request that matches the forwarding rule.

Table 5-566 RemoveHeaderConfig

Parameter	Type	Description
key	String	Specifies the key of the header you want to remove from the request that matches the forwarding rule. The value is a string of 1 to 40 case-insensitive characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. The key cannot be the following: connection, upgrade, content-length, transfer-encoding, keep-alive, te, host, cookie, remoteip, authority, x-forwarded-host, x-forwarded-for, x-forwarded-for-port, x-forwarded-tls-certificate-id, x-forwarded-tls-protocol, x-forwarded-tls-cipher, x-forwarded-elb-ip, x-forwarded-port, x-forwarded-elb-id, x-forwarded-elb-vip, x-real-ip, x-forwarded-proto, x-nuwa-trace-ne-in, or x-nuwa-trace-ne-out.

Table 5-567 TrafficLimitConfig

Parameter	Type	Description
qps	Integer	Specifies the maximum number of queries per second (QPS). The value ranges from **0** to **100000**. **0** indicates that QPS is not limited.

Parameter	Type	Description
per_source_ip_qps	Integer	Specifies the maximum number of queries per second (QPS) from a source IP address. This parameter is not available for QUIC listeners. The value can be **0** or **null**. The value ranges from **0** to **100000**. **0** indicates that QPS is not limited. If **qps** is not set to **0**, **per_source_ip_qps** must be specified a smaller value than **qps**.
burst	Integer	Specifies the maximum number of queries per second (QPS) from a source IP address. The value ranges from **0** to **100000**. If the number of requests exceeds the value specified for **qps** but not reaches the value specified for **burst**, 503 status code will not be returned.

Example Requests

Querying the details of a forwarding policy

```
GET https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/l7policies/cf4360fd-8631-41ff-a6f5-b72c35da74be
```

Example Responses

Status code: 200

Successful request.

```
{
  "l7policy" : {
    "redirect_pool_id" : "768e9e8c-e7cb-4fef-b24b-af9399dbb240",
    "description" : "",
    "admin_state_up" : true,
    "rules" : [ {
      "id" : "c5c2d625-676b-431e-a4c7-c59cc2664881"
    } ],
    "project_id" : "7a9941d34fc1497d8d0797429ecfd354",
    "listener_id" : "cdb03a19-16b7-4e6b-bfec-047aeec74f56",
    "redirect_url" : null,
    "redirect_url_config" : null,
    "redirect_pools_config" : {
      "pool_id" : "722e9e8c-e7cb-4fef-b24b-af9399dbb240",
      "weight" : 12
    },
    "redirect_pools_sticky_session_config" : {
      "timeout" : 23,
      "enable" : false
    },
    "fixed_response_config" : {
```



```
    "content_type" : "text/plain",
    "message_body" : "",
    "status_code" : "207"
  },
  "redirect_listener_id" : null,
  "action" : "REDIRECT_TO_POOL",
  "position" : 100,
  "priority" : 1,
  "provisioning_status" : "ACTIVE",
  "id" : "01832d99-bbd8-4340-9d0c-6ff8f7a37307",
  "name" : "l7policy-67"
 },
 "request_id" : "6be83ec4-623e-4840-a417-2fcdf8ad5dfa"
}
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ShowL7PolicySolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowL7PolicyRequest request = new ShowL7PolicyRequest();
        request.withL7policyId("{l7policy_id}");
        try {
            ShowL7PolicyResponse response = client.showL7Policy(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowL7PolicyRequest()
        request.l7policy_id = "{l7policy_id}"
        response = client.show_l7_policy(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowL7PolicyRequest{}
    request.L7policyId = "{l7policy_id}"
    response, err := client.ShowL7Policy(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	Successful request.

Error Codes

See **Error Codes**.

5.14.4 Modifying a Forwarding Policy

Function

This API is used to update a forwarding policy.

Calling Method

For details, see **Calling APIs**.

URI

PUT /v3/{project_id}/elb/l7policies/{l7policy_id}

Table 5-568 Path Parameters

Parameter	Mandatory	Type	Description
l7policy_id	Yes	String	Specifies the forwarding policy ID.

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Request Parameters

Table 5-569 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Table 5-570 Request body parameters

Parameter	Mandatory	Type	Description
l7policy	Yes	**UpdateL7PolicyOption** object	Specifies the forwarding policy.

Table 5-571 UpdateL7PolicyOption

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Specifies the administrative status of the forwarding policy. Note: The value can only be **true**.
description	No	String	Provides supplementary information about the forwarding policy.
name	No	String	Specifies the forwarding policy name.

Parameter	Mandatory	Type	Description
redirect_listener_id	No	String	Specifies the ID of the listener to which requests are redirected. Note: • This parameter cannot be updated or be **null** when **action** is set to **REDIRECT_TO_LISTENER**. • The listener's protocol must be **HTTPS** or **TERMINATED_HTTPS**. • A listener added to another load balancer is not allowed. • This parameter cannot be passed in the API for adding or updating a forwarding policy if **action** is set to **REDIRECT_TO_POOL**.
redirect_pool_id	No	String	Specifies the ID of the backend server group that requests will be forwarded to. Note: • The specified backend server group cannot be the default backend server group associated with the listener, or any backend server group associated with the forwarding policies of other listeners. • This parameter is valid when **action** is set to **REDIRECT_TO_POOL**. This parameter cannot be updated and cannot be **null**. • If this parameter is specified when **action** is set to **REDIRECT_TO_LISTENER**, an error will be reported.

Parameter	Mandatory	Type	Description
redirect_pools_config	No	Array of **UpdateRedirectPoolsConfig** objects	Specifies the backend server groups that the requests are forwarded to. Note: A maximum of 5 backend server groups can be configured for a forwarding policy.
redirect_pools_sticky_session_config	No	**UpdateRedirectPoolsStickySessionConfig** object	Specifies whether to enable sticky session for backend server groups configured for a forwarding policy. The load balancer generates a cookie after it receives a request from a client. All subsequent requests with the same cookie are routed to the same backend server groups. This parameter is unsupported for shared load balancers. If it is passed, an error will be returned.

Parameter	Mandatory	Type	Description
redirect_url_config	No	**UpdateRedirectUrlConfig** object	Specifies the URL to which requests are forwarded. Note: • This parameter will take effect only when advanced forwarding is enabled (**enhance_l7policy_enable** is set to **true**). If it is passed when **enhance_l7policy_enable** is set to **false**, an error will be returned. • This parameter is mandatory when **action** is set to **REDIRECT_TO_URL**. It cannot be specified if the value of **action** is not **REDIRECT_TO_URL**. • For shared load balancers, this parameter is unsupported. If it is passed, an error will be returned. • At least one of the four parameters (**protocol**, **host**, **port**, and **path**) must be passed, or their values cannot be set to **${xxx}** at the same time. **${xxx}** indicates that the value in the request will be used. For example, **${host}** indicates the host in the URL to be redirected. • The values of **protocol** and **port** cannot be the same as those of the associated listener, and either **host** or **path** must be passed or their values cannot be **${xxx}** at the same time. Value format: *protocol://host:port/path?query*

Parameter	Mandatory	Type	Description
fixed_response_config	No	**UpdateFixtedResponseConfig** object	Specifies the configuration of the page that will be returned. Note: • This parameter will take effect when **enhance_l7policy_enable** is set to **true**. If this parameter is passed and **enhance_l7policy_enable** is set to **false**, an error will be returned. • This parameter is mandatory when **action** is set to **FIXED_RESPONSE**. It cannot be specified if the value of **action** is not **FIXED_RESPONSE**. • For shared load balancers, this parameter is unsupported. If it is passed, an error will be returned.
redirect_pools_extend_config	No	**UpdateRedirectPoolsExtendConfig** object	Specifies the backend server group that the requests are forwarded to.
rules	No	Array of **CreateRuleOption** objects	Lists the forwarding rules in the forwarding policy. Note: • Each list can contain a maximum of 10 forwarding rules (if **conditions** is specified, a condition is considered as a rule). If **type** is set to **HOST_NAME**, **PATH**, **METHOD**, or **SOURCE_IP**, only one forwarding rule can be created for each type. • The entire list will be replaced if you update it.

Parameter	Mandatory	Type	Description
priority	No	Integer	Specifies the forwarding policy priority. A smaller value indicates a higher priority. Value ranges: • If **action** is set to **REDIRECT_TO_LISTENER**, the priority ranges from 0 to 10,000. • If **action** is set to other values, the priority ranges from 1 to 10,000. Default value options: • If this parameter is not passed and **enhance_l7policy_enable** is set to **false**, the priority of the new forwarding policy is **1**. • If **action** is set to **REDIRECT_TO_LISTENER**, the priority of the new forwarding policy is **0**. • If **action** is set to other values, the priority of the new forwarding policy will be a sum of 1 and the highest priority of existing forwarding policy in the same listener by default. – If no forwarding policies exist, the priority of the new forwarding policy will be **1** by default. – If the highest priority of existing forwarding policies is the maximum value (10,000), the forwarding policy will fail to be created because the final priority for creating the forwarding policy is the sum of 1 and 10,000, which exceeds the maximum value. In this case, specify a value or adjust the priorities of

Parameter	Mandatory	Type	Description
			existing forwarding policies. Note: • The value must be unique for forwarding policies of the same listener. • This parameter takes effect only when **enhance_l7policy_enable** is set to **true**. If this parameter is passed and **enhance_l7policy_enable** is set to **false**, an error will be returned. • If **enhance_l7policy_enable** is not enabled, forwarding policies are automatically prioritized based on the original policy sorting logic. The priorities of domain names are independent from each other. For the same domain name, the priorities are sorted in the order of exact match (**EQUAL_TO**), prefix match (**STARTS_WITH**), and regular expression match (**REGEX**). If the matching types are the same, the longer the path is, the higher the priority is. If a forwarding policy contains only a domain name without a path specified, the path is **/**, and prefix match is used by default. This parameter is supported by forwarding policies of shared load balancers.

Table 5-572 UpdateRedirectPoolsConfig

Parameter	Mandatory	Type	Description
pool_id	Yes	String	Specifies the ID of the backend server group.
weight	No	String	Specifies the weight of the backend server group. The value ranges from **0** to **100**. Requests are routed to backend server groups based on their weights. Backend server groups with higher weights receive proportionately more requests. No requests will be routed to a backend server group with a weight of 0.

Table 5-573 UpdateRedirectPoolsStickySessionConfig

Parameter	Mandatory	Type	Description
enable	No	Boolean	Specifies whether to enable sticky session for backend server groups configured in a forwarding policy. The default value is **false**, indicating that sticky session is disabled.
timeout	No	Integer	Specifies the duration that a session persists. The value ranges from **1** to **1440** (default), in minutes.

Table 5-574 UpdateRedirectUrlConfig

Parameter	Mandatory	Type	Description
protocol	No	String	Specifies the protocol for redirection. The value can be **HTTP**, **HTTPS**, or **${protocol}**. **${protocol}** indicates that the protocol of the request will be used.

Parameter	Mandatory	Type	Description
host	No	String	Specifies the name of the host that requests are redirected to. The value can contain only letters, digits, hyphens (-), and periods (.) and must start with a letter or digit. The default value is **${host}**, indicating that the host of the request will be used.
port	No	String	Specifies the port that requests are redirected to. The default value is **${port}**, indicating that the port of the request will be used.
path	No	String	Specifies the path that requests are redirected to. The value can contain only letters, digits, and special characters: _~';@^-%#&$.* +?,=!:|\/()[]{} and must start with a slash (/). $1, $2, $3, and all the way to $9 match the wildcard asterisk (*) in the request URL. The default value is **${path}**, indicating that the path of the request will be used.

Parameter	Mandatory	Type	Description
query	No	String	Specifies the query string set in the URL for redirection. The value is case-sensitive and can contain only letters, digits, and special characters: !$&'()* +,-./:;=?@^_`. $1, $2, $3, and all the way to $9 match the wildcard asterisk (*) in the request URL. The default value is **${query}**, indicating that the query string of the request will be used. For example, in the URL **https://www.example.com:8080/elb?type=loadbalancer**, **${query}** indicates **type=loadbalancer**. If this parameter is set to **${query}&name=my_name**, the URL will be redirected to **https://www.example.com:8080/elb?type=loadbalancer&name=my_name**.
status_code	No	String	Specifies the status code returned after the requests are redirected. The value can be **301**, **302**, **303**, **307**, or **308**.
insert_headers_config	No	**UpdateInsertHeadersConfig** object	Specifies the headers you want to write into the request that matches the forwarding rule.
remove_headers_config	No	**UpdateRemoveHeadersConfig** object	Specifies the headers you want to remove from the request that matches the forwarding rule.

Table 5-575 UpdateFixtedResponseConfig

Parameter	Mandatory	Type	Description
status_code	No	String	Specifies the HTTP status code configured in the forwarding rule. The value can be any integer in the range of 200–299, 400–499, or 500–599.
content_type	No	String	Specifies the format of the response body. The value can be **text/plain**, **text/css**, **text/html**, **application/javascript**, or **application/json**.
message_body	No	String	Specifies the content of the response message body.
insert_headers_config	No	**UpdateInsertHeadersConfig** object	Specifies the headers you want to write into the request that matches the forwarding rule.
remove_headers_config	No	**UpdateRemoveHeadersConfig** object	Specifies the headers you want to remove from the request that matches the forwarding rule.
traffic_limit_config	No	**UpdateTrafficLimitConfig** object	Specifies how requests are limited.

Table 5-576 UpdateRedirectPoolsExtendConfig

Parameter	Mandatory	Type	Description
rewrite_url_enable	No	Boolean	Specifies whether to set **rewrite_url_enable** to **true**.
rewrite_url_config	No	**UpdateRewriteUrlConfig** object	Specifies the URL for the backend server group that requests are forwarded to. This parameter takes effect only when **action** is set to **REDIRECT_TO_POOL**.
insert_headers_config	No	**UpdateInsertHeadersConfig** object	Specifies the headers you want to write into the request that matches the forwarding rule.

Parameter	Mandatory	Type	Description
remove_headers_config	No	**UpdateRemoveHeadersConfig** object	Specifies the headers you want to remove from the request that matches the forwarding rule.
traffic_limit_config	No	**UpdateTrafficLimitConfig** object	Specifies how requests are limited.
cors_config	No	**CreateCorsConfig** object	Specifies the CORS configurations.

Table 5-577 UpdateRewriteUrlConfig

Parameter	Mandatory	Type	Description
host	No	String	Specifies the domain name of the host that requests are redirected to. The domain name can contain only letters, digits, hyphens (-), and periods (.), and must start with a letter or digit. The default value is **${host}**, indicating that the host of the request will be used.

Parameter	Mandatory	Type	Description
path	No	String	Specifies the path that requests are redirected to. The value can contain only letters, digits, and special characters: _~';@^-%#& $.+?,=!:|/() and must start with a slash (/). $1, $2, $3, and all the way to $9 match the wildcard asterisk (*) in the request URL. If the number of regular expression match groups is less than the specified number, **${path}** is empty. If the dollar sign ($) is followed by a letter, the matching result is empty until the next special character appears, for example, **$abc#123**, and the matching result is **#123**. If the dollar sign ($) is followed by a special character, for example, **$#**, the matching result is **$#**.

Parameter	Mandatory	Type	Description
query	No	String	Specifies the query string set in the URL for redirection. The value is case-sensitive and can contain only letters, digits, and special characters: !$&'() *+,-./:;=?@^_`. $1, $2, $3, and all the way to $9 match the wildcard asterisk ()* in the request URL. The default value is **${query}**, indicating that the query string of the request will be used. If the number of regular expression match groups is less than the specified number, **${path}** is empty. If the dollar sign ($) is followed by a letter, the matching result is empty until the next special character appears, for example, **$abc#123**, and the matching result is **#123**. If the dollar sign ($) is followed by a special character, for example, **$#**, the matching result is **$#**.

Table 5-578 UpdateInsertHeadersConfig

Parameter	Mandatory	Type	Description
configs	Yes	Array of **UpdateInsertHeaderConfig** objects	Specifies the headers you want to write into the request that matches the forwarding rule.

Table 5-579 UpdateInsertHeaderConfig

Parameter	Mandatory	Type	Description
key	Yes	String	Specifies the key of the header you want to write into the request that matches the forwarding rule. The value is a string of 1 to 40 case-insensitive characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. The key cannot be the following: connection, upgrade, content-length, transfer-encoding, keep-alive, te, host, cookie, remoteip, authority, x-forwarded-host, x-forwarded-for, x-forwarded-for-port, x-forwarded-tls-certificate-id, x-forwarded-tls-protocol, x-forwarded-tls-cipher, x-forwarded-elb-ip, x-forwarded-port, x-forwarded-elb-id, x-forwarded-elb-vip, x-real-ip, x-forwarded-proto, x-nuwa-trace-ne-in, or x-nuwa-trace-ne-out.
value_type	Yes	String	Specifies the value type of the header. The value can be **USER_DEFINED**, **REFERENCE_HEADER**, or **SYSTEM_DEFINED**.

Parameter	Mandatory	Type	Description
value	Yes	String	Specifies the value of the header. If **value_type** is set to **SYSTEM_DEFINED**, the value can be **CLIENT-PORT**, **CLIENT-IP**, **ELB-PROTOCOL**, **ELB-ID**, **ELB-PORT**, **ELB-EIP**, or **ELB-VIP**. The value can contain 1 to 128 characters. ASCII codes 32 through 127 printable characters, asterisk (*), and question mark (?) are also supported. The value cannot start or end with a space.

Table 5-580 UpdateRemoveHeadersConfig

Parameter	Mandatory	Type	Description
configs	Yes	Array of **UpdateRemoveHeaderConfig** objects	Specifies the headers you want to remove from the request that matches the forwarding rule.

Table 5-581 UpdateRemoveHeaderConfig

Parameter	Mandatory	Type	Description
key	Yes	String	Specifies the key of the header you want to remove from the request that matches the forwarding rule. The value is a string of 1 to 40 case-insensitive characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. The key cannot be the following: connection, upgrade, content-length, transfer-encoding, keep-alive, te, host, cookie, remoteip, authority, x-forwarded-host, x-forwarded-for, x-forwarded-for-port, x-forwarded-tls-certificate-id, x-forwarded-tls-protocol, x-forwarded-tls-cipher, x-forwarded-elb-ip, x-forwarded-port, x-forwarded-elb-id, x-forwarded-elb-vip, x-real-ip, x-forwarded-proto, x-nuwa-trace-ne-in, or x-nuwa-trace-ne-out.

Table 5-582 UpdateTrafficLimitConfig

Parameter	Mandatory	Type	Description
qps	No	Integer	Specifies the maximum number of queries per second (QPS). The value ranges from **0** to **100000**. **0** indicates that QPS is not limited.

Parameter	Mandatory	Type	Description
per_source_ip_qps	No	Integer	Specifies the maximum number of queries per second (QPS) from a source IP address. This parameter is not available for QUIC listeners. The value can be **0** or **null**. The value ranges from **0** to **100000**. **0** indicates that QPS is not limited. If **qps** is not set to **0**, **per_source_ip_qps** must be specified a smaller value than **qps**.
burst	No	Integer	Specifies the maximum number of queries per second (QPS) from a source IP address. The value ranges from **0** to **100000**. If the number of requests exceeds the value specified for **qps** but not reaches the value specified for **burst**, 503 status code will not be returned.

Table 5-583 CreateCorsConfig

Parameter	Mandatory	Type	Description
allow_origin	No	Array of strings	Specifies the origins that are allowed to access cross-origin resources through a browser. The origin can be a wildcard (*) or one or more URLs. Constraints: • Each URL must start with **http://** or **https://**, followed by a valid domain name or level-1 wildcard domain name, for example, http://*.test.abc.example.com. • It is optional to include a port number (ranging from 1 to 65535) in the URL.

Parameter	Mandatory	Type	Description
allow_methods	No	Array of strings	Specifies the HTTP methods that the specified URLs can use to access cross-origin resources.
allow_headers	No	Array of strings	Specifies the request headers that can be carried in CORS requests.
expose_headers	No	Array of strings	Specifies the headers that can be exposed.
allow_credentials	No	Boolean	Specifies whether to allow credentials in CORS requests. Value options: • **true**: Credentials are allowed. • **false**: Credentials are not allowed.
max_age	No	Long	Specifies the maximum duration a preflight request can be cached, in seconds. Value range: -1 to 172800

Table 5-584 CreateRuleOption

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Specifies the administrative status of the forwarding rule. The value can only be **true**.

Parameter	Mandatory	Type	Description
compare_type	Yes	String	Specifies how requests are matched with the forwarding rule. Value options: • **EQUAL_TO**: exact match. • **REGEX**: regular expression match • **STARTS_WITH**: prefix match Note: • If **type** is set to **HOST_NAME**, the value can only be **EQUAL_TO**, and asterisks (*) can be used as wildcard characters. • If **type** is set to **PATH**, the value can be **REGEX**, **STARTS_WITH**, or **EQUAL_TO**. • If **type** is set to **METHOD** or **SOURCE_IP**, the value can only be **EQUAL_TO**. • If **type** is set to **HEADER** or **QUERY_STRING**, the value can only be **EQUAL_TO**, asterisks (*) and question marks (?) can be used as wildcard characters.
key	No	String	Specifies the key of match content. For example, if the request header is used for forwarding, **key** is the request header. This parameter is unsupported. Please do not use it.

Parameter	Mandatory	Type	Description
value	Yes	String	Specifies the value of the match item. For example, if a domain name is used for matching, **value** is the domain name. Note: • This parameter will take effect only when **conditions** is left blank. • If **type** is set to **HOST_NAME**, the value can contain letters, digits, hyphens (-), and periods (.) and must start with a letter or digit. If you want to use a wildcard domain name, enter an asterisk (*) as the leftmost label of the domain name. • If **type** is set to **PATH** and **compare_type** to **STARTS_WITH** or **EQUAL_TO**, the value must start with a slash (/) and can contain only letters, digits, and special characters _~';@^-%#&$.*+?,=!:|\/()[]{} • If **type** is set to **METHOD**, **SOURCE_IP**, **HEADER**, or **QUERY_STRING**, this parameter will not take effect, and **conditions** will be used to specify the key and value.
project_id	No	String	Specifies the project ID.

Parameter	Mandatory	Type	Description
type	Yes	String	Specifies the type of the forwarding rule. Value options: • **HOST_NAME**: A domain name will be used for matching. • **PATH**: A URL will be used for matching. • **METHOD**: An HTTP request method will be used for matching. • **HEADER**: The request header will be used for matching. • **QUERY_STRING**: A query string will be used for matching. • **SOURCE_IP**: The source IP address will be used for matching. • **COOKIE**: The cookie will be used for matching. Note: If **type** is set to **HOST_NAME**, **PATH**, **METHOD**, or **SOURCE_IP**, only one forwarding rule can be created for each type. If **type** is set to **HEADER** and **QUERY_STRING**, multiple forwarding rules can be created for each type.
invert	No	Boolean	Specifies whether reverse matching is supported. Value range: **true** or **false** Default value: **false** This parameter is unsupported. Please do not use it.

Parameter	Mandatory	Type	Description
conditions	No	Array of **CreateRuleCondition** objects	Specifies the conditions contained in a forwarding rule. Note: • This parameter will take effect when **enhance_l7policy_enable** is set to **true**. • If **conditions** is specified, **key** and **value** will not take effect. • The keys in the list must be the same, whereas each value must be unique.

Table 5-585 CreateRuleCondition

Parameter	Mandatory	Type	Description
key	No	String	Specifies the key of match item. Note: • All keys in the conditions list in the same rule must be the same. • If **type** is set to **HOST_NAME**, **PATH**, **METHOD**, or **SOURCE_IP**, this parameter is an empty string. • If **type** is set to **HEADER**, **key** indicates the name of the HTTP header parameter, and **value** indicates the value of the request header parameter. The value can contain 1 to 40 characters, including letters, digits, hyphens (-), and underscores (_). • If **type** is set to **QUERY_STRING**, **key** indicates the name of the query parameter, and **value** indicates the value of the query parameter. The key is case sensitive and can contain 1 to 128 characters. Spaces, square brackets ([ ]), curly brackets ({ }), angle brackets (< >), backslashes (), double quotation marks (" "), pound signs (#), ampersands (&), vertical bars (|), percent signs (%), and tildes (~) are not supported.

Parameter	Mandatory	Type	Description
value	Yes	String	Specifies the value of the match item. Note: • The key of each condition in a forwarding policy must be the same. • The value of each condition in a forwarding policy must be unique. Value ranges: • If **type** is set to **HOST_NAME**, **key** is left blank, **value** indicates the domain name, which can contain 1 to 128 characters, including letters, digits, hyphens (-), periods (.), and asterisks (*), and must start with a letter, digit, or asterisk (*). If you want to use a wildcard domain name, enter an asterisk (*) as the leftmost label of the domain name. • If **type** is set to **PATH**, **key** is left blank, **value** indicates the request path, which can contain 1 to 128 characters. If **compare_type** is set to **STARTS_WITH** or **EQUAL_TO** for the forwarding rule, the value must start with a slash (/) and can contain only letters, digits, and special characters: _~';@^-%#&$.*+?,=!:|/()[]{} • If **type** is set to **HEADER**, **key** indicates the name of the HTTP header parameter and **value** indicates the value of the HTTP header parameter. The value can contain 1 to 128 characters. Asterisks (*) and question marks (?) are allowed, but spaces and double

Parameter	Mandatory	Type	Description
			quotation marks are not allowed. An asterisk can match zero or more characters, and a question mark can match 1 character. • If **type** is set to **QUERY_STRING**, **key** indicates the name of the query parameter and **value** indicates the value of the query parameter. The value is case sensitive and can contain 1 to 128 characters. Spaces, square brackets ([ ]), curly brackets ({ }), angle brackets (< >), backslashes (), double quotation marks (" "), pound signs (#), ampersands (&), vertical bars (|), percent signs (%), and tildes (~) are not supported. Asterisks (*) and question marks (?) are allowed. An asterisk can match zero or more characters, and a question mark can match 1 character. • If **type** is set to **METHOD**, **key** is left blank, **value** indicates the HTTP method. The value can be **GET**, **PUT**, **POST**, **DELETE**, **PATCH**, **HEAD**, or **OPTIONS**. • If **type** is set to **SOURCE_IP**, **key** is left blank, **value** indicates the source IP address of the request. The value is an IPv4 or IPv6 CIDR block, for example, 192.168.0.2/32 or 2049::49/64.

Response Parameters

Status code: 200

Table 5-586 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
l7policy	**L7Policy** object	Specifies the forwarding policy.

Table 5-587 L7Policy

Parameter	Type	Description
action	String	Specifies where requests will be forwarded. Value options: • **REDIRECT_TO_POOL**: Requests will be forwarded to another backend server group. • **REDIRECT_TO_LISTENER**: Requests will be redirected to an HTTPS listener. • **REDIRECT_TO_URL**: Requests will be redirected to another URL. • **FIXED_RESPONSE**: A fixed response body will be returned. Note: • **REDIRECT_TO_LISTENER** has the highest priority. If requests are to be redirected to an HTTPS listener, other forwarding policies of the listener will become invalid. • If **action** is set to **REDIRECT_TO_POOL**, the listener's protocol must be HTTP, HTTPS, or TERMINATED_HTTPS. • If **action** is set to **REDIRECT_TO_LISTENER**, the listener's protocol must be HTTP.
admin_state_up	Boolean	Specifies the administrative status of the forwarding policy. Note: The value can only be **true**.
description	String	Provides supplementary information about the forwarding policy.
id	String	Specifies the forwarding policy ID.

Parameter	Type	Description
listener_id	String	Specifies the ID of the listener to which the forwarding policy is added.
name	String	Specifies the forwarding policy name.
position	Integer	Specifies the forwarding policy priority. This parameter cannot be updated. This parameter is unsupported. Please do not use it.

Parameter	Type	Description
priority	Integer	Specifies the forwarding policy priority. A smaller value indicates a higher priority. Value ranges: • If **action** is set to **REDIRECT_TO_LISTENER**, the priority ranges from 0 to 10,000. • If **action** is set to other values, the priority ranges from 1 to 10,000. Default value options: • If this parameter is not passed and **enhance_l7policy_enable** is set to **false**, the priority of the new forwarding policy is **1**. • If **action** is set to **REDIRECT_TO_LISTENER**, the priority of the new forwarding policy is **0**. • If **action** is set to other values, the priority of the new forwarding policy will be a sum of 1 and the highest priority of existing forwarding policy in the same listener by default. – If no forwarding policies exist, the priority of the new forwarding policy will be **1** by default. – If the highest priority of existing forwarding policies is the maximum value (10,000), the forwarding policy will fail to be created because the final priority for creating the forwarding policy is the sum of 1 and 10,000, which exceeds the maximum value. In this case, specify a value or adjust the priorities of existing forwarding policies. Note: • The value must be unique for forwarding policies of the same listener. • This parameter takes effect only when **enhance_l7policy_enable** is

Parameter	Type	Description
		set to **true**. If this parameter is passed and **enhance_l7policy_enable** is set to **false**, an error will be returned. • If **enhance_l7policy_enable** is not enabled, forwarding policies are automatically prioritized based on the original policy sorting logic. The priorities of domain names are independent from each other. For the same domain name, the priorities are sorted in the order of exact match (**EQUAL_TO**), prefix match (**STARTS_WITH**), and regular expression match (**REGEX**). If the matching types are the same, the longer the path is, the higher the priority is. If a forwarding policy contains only a domain name without a path specified, the path is **/**, and prefix match is used by default. This parameter is supported by forwarding policies of shared load balancers.
project_id	String	Specifies the project ID of the forwarding policy.
provisioning_status	String	Specifies the provisioning status of the forwarding policy. The value can be **ACTIVE** or **ERROR**. • **ACTIVE** (default): The forwarding policy is provisioned successfully. • **ERROR**: Another forwarding policy of the same listener has the same forwarding rule.
redirect_pool_id	String	Specifies the ID of the backend server group to which the requests are forwarded. Note: This parameter is valid only when **action** is set to **REDIRECT_TO_POOL**.

Parameter	Type	Description
redirect_listener_id	String	Specifies the ID of the listener to which requests are redirected. Note: • This parameter is mandatory when **action** is set to **REDIRECT_TO_LISTENER**. • The listener's protocol must be **HTTPS** or **TERMINATED_HTTPS**. • A listener added to another load balancer is not allowed. • This parameter cannot be passed in the API for adding or updating a forwarding policy if **action** is set to **REDIRECT_TO_POOL**.
redirect_url	String	Specifies the URL to which requests are forwarded. Format: *protocol://host:port/path?query* This parameter is unsupported. Please do not use it.
rules	Array of **RuleRef** objects	Lists the forwarding rules in the forwarding policy.

Parameter	Type	Description
redirect_url_config	**RedirectUrlConfig** object	Specifies the URL to which requests are forwarded. Note: • This parameter will take effect only when advanced forwarding is enabled (**enhance_l7policy_enable** is set to **true**). If it is passed when **enhance_l7policy_enable** is set to **false**, an error will be returned. • This parameter is mandatory when **action** is set to **REDIRECT_TO_URL**. It cannot be specified if the value of **action** is not **REDIRECT_TO_URL**. • For shared load balancers, this parameter is unsupported. If it is passed, an error will be returned. • At least one of the four parameters (**protocol**, **host**, **port**, and **path**) must be passed, or their values cannot be set to **${xxx}** at the same time. **${xxx}** indicates that the value in the request will be used. For example, **${host}** indicates the host in the URL to be redirected. • The values of **protocol** and **port** cannot be the same as those of the associated listener, and either **host** or **path** must be passed or their values cannot be **${xxx}** at the same time. Value format: *protocol://host:port/path?query*
redirect_pools_config	Array of **RedirectPoolsConfig** objects	Specifies the backend server groups that the requests are forwarded to. Note: A maximum of 5 backend server groups can be configured for a forwarding policy.

Parameter	Type	Description
redirect_pools_sticky_session_config	**RedirectPoolsStickySessionConfig** object	Specifies whether to enable sticky session for backend server groups configured for a forwarding policy. The load balancer generates a cookie after it receives a request from a client. All subsequent requests with the same cookie are routed to the same backend server groups. This parameter is unsupported for shared load balancers. If it is passed, an error will be returned.
redirect_pools_extend_config	**RedirectPoolsExtendConfig** object	Specifies the backend server group that requests are forwarded to. Note: This parameter takes effect only when **action** is set to **REDIRECT_TO_POOL**.
fixed_response_config	**FixtedResponseConfig** object	Specifies the configuration of the page that will be returned. Note: • This parameter will take effect when **enhance_l7policy_enable** is set to **true**. If this parameter is passed and **enhance_l7policy_enable** is set to **false**, an error will be returned. • This parameter is mandatory when **action** is set to **FIXED_RESPONSE**. It cannot be specified if the value of **action** is not **FIXED_RESPONSE**. • For shared load balancers, this parameter is unsupported. If it is passed, an error will be returned.
created_at	String	Specifies the time when the forwarding policy was added. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.

Parameter	Type	Description
updated_at	String	Specifies the time when the forwarding policy was updated. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
enterprise_project_id	String	Specifies the ID of the enterprise project.

Table 5-588 RuleRef

Parameter	Type	Description
id	String	Specifies the forwarding rule ID.

Table 5-589 RedirectUrlConfig

Parameter	Type	Description
protocol	String	Specifies the protocol for redirection. The value can be **HTTP**, **HTTPS**, or **${protocol}**. **${protocol}** indicates that the protocol of the request will be used.
host	String	Specifies the name of the host that requests are redirected to. The value can contain only letters, digits, hyphens (-), and periods (.) and must start with a letter or digit. The default value is **${host}**, indicating that the host of the request will be used.
port	String	Specifies the port that requests are redirected to. The default value is **${port}**, indicating that the port of the request will be used.

Parameter	Type	Description
path	String	Specifies the path that requests are redirected to. The value can contain only letters, digits, and special characters: _~';@^-%#&$.*+?,=!:|\/()[]{} and must start with a slash (/). $1, $2, $3, and all the way to $9 match the wildcard asterisk (*) in the request URL. The default value is **${path}**, indicating that the path of the request will be used.
query	String	Specifies the query string set in the URL for redirection. The value is case-sensitive and can contain only letters, digits, and special characters: !$&'()*+,-./:;=?@^_`. $1, $2, $3, and all the way to $9 match the wildcard asterisk (*) in the request URL. The default value is **${query}**, indicating that the query string of the request will be used. For example, in the URL **https://www.example.com:8080/elb?type=loadbalancer**, **${query}** indicates **type=loadbalancer**. If this parameter is set to **${query}&name=my_name**, the URL will be redirected to **https://www.example.com:8080/elb?type=loadbalancer&name=my_name**.
status_code	String	Specifies the status code returned after the requests are redirected. The value can be **301**, **302**, **303**, **307**, or **308**.
insert_headers_config	**InsertHeadersConfig** object	Specifies the headers you want to write into the request that matches the forwarding rule.
remove_headers_config	**RemoveHeadersConfig** object	Specifies the headers you want to remove from the request that matches the forwarding rule.

Table 5-590 RedirectPoolsConfig

Parameter	Type	Description
pool_id	String	Specifies the ID of the backend server group.
weight	Integer	Specifies the weight of the backend server group. The value ranges from **0** to **100**. Requests are routed to backend server groups based on their weights. Backend server groups with higher weights receive proportionately more requests. No requests will be routed to a backend server group with a weight of 0.

Table 5-591 RedirectPoolsStickySessionConfig

Parameter	Type	Description
enable	Boolean	Specifies whether to enable sticky session for backend server groups configured in a forwarding policy. The default value is **false**, indicating that sticky session is disabled.
timeout	Integer	Specifies the duration that a session persists. The value ranges from **1** to **1440** (default), in minutes.

Table 5-592 RedirectPoolsExtendConfig

Parameter	Type	Description
rewrite_url_enable	Boolean	Specifies whether to set **rewrite_url_enable** to **true**.
rewrite_url_config	**RewriteUrlConfig** object	Specifies the URL for the backend server group that requests are forwarded to. This parameter takes effect only when **action** is set to **REDIRECT_TO_POOL**.
insert_headers_config	**InsertHeadersConfig** object	Specifies the headers you want to write into the request that matches the forwarding rule.

Parameter	Type	Description
remove_headers_config	**RemoveHeadersConfig** object	Specifies the headers you want to remove from the request that matches the forwarding rule.
traffic_limit_config	**TrafficLimitConfig** object	Specifies how requests are limited.
cors_config	**CorsConfig** object	Specifies the CORS configurations.

Table 5-593 RewriteUrlConfig

Parameter	Type	Description
host	String	Specifies the domain name of the host that requests are redirected to. The domain name can contain only letters, digits, hyphens (-), and periods (.), and must start with a letter or digit. The default value is **${host}**, indicating that the host of the request will be used.
path	String	Specifies the path that requests are redirected to. The default value is **${path}**, indicating that the path of the request will be used. The value can contain only letters, digits, and special characters: _~';@^-%#&$.+?,=!:|/() and must start with a slash (/). $1, $2, $3, and all the way to $9 match the wildcard asterisk (*) in the request URL. If the number of regular expression match groups is less than the specified number, **${path}** is empty. If the dollar sign ($) is followed by a letter, the matching result is empty until the next special character appears, for example, **$abc#123**, and the matching result is **#123**. If the dollar sign ($) is followed by a special character, for example, **$#**, the matching result is **$#**.

Parameter	Type	Description
query	String	Specifies the query string set in the URL for redirection. The value is case-sensitive and can contain only letters, digits, and special characters: !$&'()*+,-./:;=?@^_`. *$1, $2, $3, and all the way to $9 match the wildcard asterisk (*)* in the request URL. The default value is **${query}**, indicating that the query string of the request will be used. If the number of regular expression match groups is less than the specified number, **${path}** is empty. If the dollar sign ($) is followed by a letter, the matching result is empty until the next special character appears, for example, **$abc#123**, and the matching result is **#123**. If the dollar sign ($) is followed by a special character, for example, **$#**, the matching result is **$#**.

Table 5-594 CorsConfig

Parameter	Type	Description
allow_origin	Array of strings	Specifies the origins that are allowed to access cross-origin resources through a browser. The origin can be a wildcard (*) or one or more URLs. Constraints: • Each URL must start with **http://** or **https://**, followed by a valid domain name or level-1 wildcard domain name, for example, http://*.test.abc.example.com. • It is optional to include a port number (ranging from 1 to 65535) in the URL.
allow_methods	Array of strings	Specifies the HTTP methods that the specified URLs can use to access cross-origin resources.
allow_headers	Array of strings	Specifies the request headers that can be carried in CORS requests.
expose_headers	Array of strings	Specifies the headers that can be exposed.

Parameter	Type	Description
allow_credentials	Boolean	Specifies whether to allow credentials in CORS requests. Value options: • **true**: Credentials are allowed. • **false**: Credentials are not allowed.
max_age	Long	Specifies the maximum duration a preflight request can be cached, in seconds. Value range: -1 to 172800

Table 5-595 FixtedResponseConfig

Parameter	Type	Description
status_code	String	Specifies the HTTP status code configured in the forwarding policy. The value can be any integer in the range of 200–299, 400–499, or 500–599.
content_type	String	Specifies the format of the response body. The value can be **text/plain**, **text/css**, **text/html**, **application/javascript**, or **application/json**.
message_body	String	Specifies the content of the response message body.
insert_headers_config	**InsertHeadersConfig** object	Specifies the headers you want to write into the request that matches the forwarding rule.
remove_headers_config	**RemoveHeadersConfig** object	Specifies the headers you want to remove from the request that matches the forwarding rule.
traffic_limit_config	**TrafficLimitConfig** object	Specifies how requests are limited.

Table 5-596 InsertHeadersConfig

Parameter	Type	Description
configs	Array of **InsertHeaderConfig** objects	Specifies the headers you want to write into the request that matches the forwarding rule.

Table 5-597 InsertHeaderConfig

Parameter	Type	Description
key	String	Specifies the key of the header you want to write into the request that matches the forwarding rule. The value is a string of 1 to 40 case-insensitive characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. The key cannot be the following: connection, upgrade, content-length, transfer-encoding, keep-alive, te, host, cookie, remoteip, authority, x-forwarded-host, x-forwarded-for, x-forwarded-for-port, x-forwarded-tls-certificate-id, x-forwarded-tls-protocol, x-forwarded-tls-cipher, x-forwarded-elb-ip, x-forwarded-port, x-forwarded-elb-id, x-forwarded-elb-vip, x-real-ip, x-forwarded-proto, x-nuwa-trace-ne-in, or x-nuwa-trace-ne-out.
value_type	String	Specifies the value type of the header. The value can be **USER_DEFINED**, **REFERENCE_HEADER**, or **SYSTEM_DEFINED**.
value	String	Specifies the value of the header. If **value_type** is set to **SYSTEM_DEFINED**, the value can be **CLIENT-PORT**, **CLIENT-IP**, **ELB-PROTOCOL**, **ELB-ID**, **ELB-PORT**, **ELB-EIP**, or **ELB-VIP**. The value can contain 1 to 128 characters. ASCII codes 32 through 127 printable characters, asterisk (*), and question mark (?) are also supported. The value cannot start or end with a space.

Table 5-598 RemoveHeadersConfig

Parameter	Type	Description
configs	Array of **RemoveHeaderConfig** objects	Specifies the headers you want to remove from the request that matches the forwarding rule.

Table 5-599 RemoveHeaderConfig

Parameter	Type	Description
key	String	Specifies the key of the header you want to remove from the request that matches the forwarding rule. The value is a string of 1 to 40 case-insensitive characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. The key cannot be the following: connection, upgrade, content-length, transfer-encoding, keep-alive, te, host, cookie, remoteip, authority, x-forwarded-host, x-forwarded-for, x-forwarded-for-port, x-forwarded-tls-certificate-id, x-forwarded-tls-protocol, x-forwarded-tls-cipher, x-forwarded-elb-ip, x-forwarded-port, x-forwarded-elb-id, x-forwarded-elb-vip, x-real-ip, x-forwarded-proto, x-nuwa-trace-ne-in, or x-nuwa-trace-ne-out.

Table 5-600 TrafficLimitConfig

Parameter	Type	Description
qps	Integer	Specifies the maximum number of queries per second (QPS). The value ranges from **0** to **100000**. **0** indicates that QPS is not limited.

Parameter	Type	Description
per_source_ip_qps	Integer	Specifies the maximum number of queries per second (QPS) from a source IP address. This parameter is not available for QUIC listeners. The value can be **0** or **null**. The value ranges from **0** to **100000**. **0** indicates that QPS is not limited. If **qps** is not set to **0**, **per_source_ip_qps** must be specified a smaller value than **qps**.
burst	Integer	Specifies the maximum number of queries per second (QPS) from a source IP address. The value ranges from **0** to **100000**. If the number of requests exceeds the value specified for **qps** but not reaches the value specified for **burst**, 503 status code will not be returned.

Example Requests

Modifying a forwarding policy

```
PUT https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/l7policies/cf4360fd-8631-41ff-a6f5-b72c35da74be

{
  "l7policy" : {
    "name" : "My policy.",
    "description" : "Update policy.",
    "redirect_listener_id" : "48a97732-449e-4aab-b561-828d29e45050"
  }
}
```

Example Responses

Status code: 200

Successful request.

```
{
  "request_id" : "e5c07525-1470-47b6-9b0c-567527a036aa",
  "l7policy" : {
    "redirect_pool_id" : "768e9e8c-e7cb-4fef-b24b-af9399dbb240",
    "description" : "",
    "admin_state_up" : true,
    "rules" : [ {
      "id" : "c5c2d625-676b-431e-a4c7-c59cc2664881"
    } ],
    "project_id" : "7a9941d34fc1497d8d0797429ecfd354",
    "listener_id" : "cdb03a19-16b7-4e6b-bfec-047aeec74f56",
    "redirect_url" : null,
    "redirect_url_config" : null,
```



```
  "redirect_pools_config" : {
    "pool_id" : "722e9e8c-e7cb-4fef-b24b-af9399dbb240",
    "weight" : 12
  },
  "redirect_pools_sticky_session_config" : {
    "timeout" : 23,
    "enable" : false
  },
  "fixed_response_config" : null,
  "redirect_listener_id" : null,
  "action" : "REDIRECT_TO_POOL",
  "position" : 100,
  "priority" : null,
  "provisioning_status" : "ACTIVE",
  "id" : "01832d99-bbd8-4340-9d0c-6ff8f7a37307",
  "name" : "l7policy-67"
 }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Modifying a forwarding policy

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class UpdateL7PolicySolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdateL7PolicyRequest request = new UpdateL7PolicyRequest();
        request.withL7policyId("{l7policy_id}");
        UpdateL7PolicyRequestBody body = new UpdateL7PolicyRequestBody();
        UpdateL7PolicyOption l7policybody = new UpdateL7PolicyOption();
        l7policybody.withDescription("Update policy.")
            .withName("My policy.")
            .withRedirectListenerId("48a97732-449e-4aab-b561-828d29e45050");
```



```
        body.withL7policy(l7policybody);
        request.withBody(body);
        try {
            UpdateL7PolicyResponse response = client.updateL7Policy(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

Modifying a forwarding policy

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdateL7PolicyRequest()
        request.l7policy_id = "{l7policy_id}"
        l7policybody = UpdateL7PolicyOption(
            description="Update policy.",
            name="My policy.",
            redirect_listener_id="48a97732-449e-4aab-b561-828d29e45050"
        )
        request.body = UpdateL7PolicyRequestBody(
            l7policy=l7policybody
        )
        response = client.update_l7_policy(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

Modifying a forwarding policy

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdateL7PolicyRequest{}
    request.L7policyId = "{l7policy_id}"
    descriptionL7policy:= "Update policy."
    nameL7policy:= "My policy."
    redirectListenerIdL7policy:= "48a97732-449e-4aab-b561-828d29e45050"
    l7policybody := &model.UpdateL7PolicyOption{
        Description: &descriptionL7policy,
        Name: &nameL7policy,
        RedirectListenerId: &redirectListenerIdL7policy,
    }
    request.Body = &model.UpdateL7PolicyRequestBody{
        L7policy: l7policybody,
    }
    response, err := client.UpdateL7Policy(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	Successful request.

Error Codes

See **Error Codes**.

5.14.5 Deleting a Forwarding Policy

Function

This API is used to delete a forwarding policy.

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v3/{project_id}/elb/l7policies/{l7policy_id}

Table 5-601 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
l7policy_id	Yes	String	Specifies the forwarding policy ID.

Request Parameters

Table 5-602 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

None

Example Requests

Delete a given forwarding policy

```
DELETE https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/l7policies/cf4360fd-8631-41ff-a6f5-b72c35da74be
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class DeleteL7PolicySolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteL7PolicyRequest request = new DeleteL7PolicyRequest();
        request.withL7policyId("{l7policy_id}");
        try {
            DeleteL7PolicyResponse response = client.deleteL7Policy(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteL7PolicyRequest()
        request.l7policy_id = "{l7policy_id}"
        response = client.delete_l7_policy(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteL7PolicyRequest{}
    request.L7policyId = "{l7policy_id}"
    response, err := client.DeleteL7Policy(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	Successful request.

Error Codes

See **Error Codes**.

5.14.6 Batch Modifying Forwarding Policy Priorities

Function

This API is used to batch modify the priorities of forwarding policies.

Constraints

This API is only used to update the priorities of forwarding policies added to a listener of a dedicated load balancer when **action** is set to **REDIRECT_TO_POOL**.

Calling Method

For details, see **Calling APIs**.

URI

POST /v3/{project_id}/elb/l7policies/batch-update-priority

Table 5-603 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Request Parameters

Table 5-604 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Table 5-605 Request body parameters

Parameter	Mandatory	Type	Description
l7policies	No	Array of **BatchUpdatePriorityRequestBody** objects	Specifies the forwarding policy.

Table 5-606 BatchUpdatePriorityRequestBody

Parameter	Mandatory	Type	Description
id	Yes	String	Specifies the ID of the forwarding policy.

Parameter	Mandatory	Type	Description
priority	Yes	Integer	Specifies the forwarding policy priority. A smaller value indicates a higher priority. Value ranges: • If **action** is set to **REDIRECT_TO_LISTENER**, the priority ranges from 0 to 10,000. • If **action** is set to other values, the priority ranges from 1 to 10,000. Default value options: • If this parameter is not passed and **enhance_l7policy_enable** is set to **false**, the priority of the new forwarding policy is **1**. • If **action** is set to **REDIRECT_TO_LISTENER**, the priority of the new forwarding policy is **0**. • If **action** is set to other values, the priority of the new forwarding policy will be a sum of 1 and the highest priority of existing forwarding policy in the same listener by default. – If no forwarding policies exist, the priority of the new forwarding policy will be **1** by default. – If the highest priority of existing forwarding policies is the maximum value (10,000), the forwarding policy will fail to be created because the final priority for creating the forwarding policy is the sum of 1 and 10,000, which exceeds the maximum value. In this case, specify a value or adjust the priorities of

Parameter	Mandatory	Type	Description
			existing forwarding policies. Note: • The value must be unique for forwarding policies of the same listener. • This parameter takes effect only when **enhance_l7policy_enable** is set to **true**. If this parameter is passed and **enhance_l7policy_enable** is set to **false**, an error will be returned. • If **enhance_l7policy_enable** is not enabled, forwarding policies are automatically prioritized based on the original policy sorting logic. The priorities of domain names are independent from each other. For the same domain name, the priorities are sorted in the order of exact match (**EQUAL_TO**), prefix match (**STARTS_WITH**), and regular expression match (**REGEX**). If the matching types are the same, the longer the path is, the higher the priority is. If a forwarding policy contains only a domain name without a path specified, the path is **/**, and prefix match is used by default. This parameter is supported by forwarding policies of shared load balancers.

Response Parameters

Status code: 202

Table 5-607 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID.

Example Requests

Batch modifying the priorities of forwarding policies

```
POST https://{ELB_Endpoint}/v3/060576782980d5762f9ec014dd2f1148/elb/l7policies/batch-update-priority

{
  "l7policies" : [ {
    "id" : "1fe93e12-6e07-47a9-8f81-3346c015601d",
    "priority" : 11
  } ]
}
```

Example Responses

Status code: 202

Created

```
{
  "request_id" : "e5c07525-1470-47b6-9b0c-567527a036aa"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Batch modifying the priorities of forwarding policies

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;

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

public class BatchUpdatePoliciesPrioritySolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        BatchUpdatePoliciesPriorityRequest request = new BatchUpdatePoliciesPriorityRequest();
        BatchUpdatePoliciesPriorityRequestBody body = new BatchUpdatePoliciesPriorityRequestBody();
        List<BatchUpdatePriorityRequestBody> listbodyL7policies = new ArrayList<>();
        listbodyL7policies.add(
            new BatchUpdatePriorityRequestBody()
                .withId("1fe93e12-6e07-47a9-8f81-3346c015601d")
                .withPriority(11)
        );
        body.withL7policies(listbodyL7policies);
        request.withBody(body);
        try {
            BatchUpdatePoliciesPriorityResponse response = client.batchUpdatePoliciesPriority(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

Batch modifying the priorities of forwarding policies

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = BatchUpdatePoliciesPriorityRequest()
        listL7policiesbody = [
```

```
            BatchUpdatePriorityRequestBody(
                id="1fe93e12-6e07-47a9-8f81-3346c015601d",
                priority=11
            )
        ]
        request.body = BatchUpdatePoliciesPriorityRequestBody(
            l7policies=listL7policiesbody
        )
        response = client.batch_update_policies_priority(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

Batch modifying the priorities of forwarding policies

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.BatchUpdatePoliciesPriorityRequest{}
    var listL7policiesbody = []model.BatchUpdatePriorityRequestBody{
        {
            Id: "1fe93e12-6e07-47a9-8f81-3346c015601d",
            Priority: int32(11),
        },
    }
    request.Body = &model.BatchUpdatePoliciesPriorityRequestBody{
        L7policies: &listL7policiesbody,
    }
    response, err := client.BatchUpdatePoliciesPriority(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
202	Created

Error Codes

See **Error Codes**.

5.15 Forwarding Rule

5.15.1 Adding a Forwarding Rule

Function

This API is used to add a forwarding rule.

Constraints

If the action of **l7policy** is set to **Redirect to another listener**, **l7rule** cannot be created.

Calling Method

For details, see **Calling APIs**.

URI

POST /v3/{project_id}/elb/l7policies/{l7policy_id}/rules

Table 5-608 Path Parameters

Parameter	Mandatory	Type	Description
l7policy_id	Yes	String	Specifies the forwarding policy ID.
project_id	Yes	String	Specifies the project ID.

Request Parameters

Table 5-609 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Table 5-610 Request body parameters

Parameter	Mandatory	Type	Description
rule	Yes	**CreateRuleOption** object	Specifies the forwarding rule.

Table 5-611 CreateRuleOption

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Specifies the administrative status of the forwarding rule. The value can only be **true**.

Parameter	Mandatory	Type	Description
compare_type	Yes	String	Specifies how requests are matched with the forwarding rule. Value options: • **EQUAL_TO**: exact match. • **REGEX**: regular expression match • **STARTS_WITH**: prefix match Note: • If **type** is set to **HOST_NAME**, the value can only be **EQUAL_TO**, and asterisks (*) can be used as wildcard characters. • If **type** is set to **PATH**, the value can be **REGEX**, **STARTS_WITH**, or **EQUAL_TO**. • If **type** is set to **METHOD** or **SOURCE_IP**, the value can only be **EQUAL_TO**. • If **type** is set to **HEADER** or **QUERY_STRING**, the value can only be **EQUAL_TO**, asterisks (*) and question marks (?) can be used as wildcard characters.
key	No	String	Specifies the key of match content. For example, if the request header is used for forwarding, **key** is the request header. This parameter is unsupported. Please do not use it.

Parameter	Mandatory	Type	Description
value	Yes	String	Specifies the value of the match item. For example, if a domain name is used for matching, **value** is the domain name. Note: • This parameter will take effect only when **conditions** is left blank. • If **type** is set to **HOST_NAME**, the value can contain letters, digits, hyphens (-), and periods (.) and must start with a letter or digit. If you want to use a wildcard domain name, enter an asterisk (*) as the leftmost label of the domain name. • If **type** is set to **PATH** and **compare_type** to **STARTS_WITH** or **EQUAL_TO**, the value must start with a slash (/) and can contain only letters, digits, and special characters _~';@^-%#&$.* +?,=!:|\/()[]{} • If **type** is set to **METHOD**, **SOURCE_IP**, **HEADER**, or **QUERY_STRING**, this parameter will not take effect, and **conditions** will be used to specify the key and value.
project_id	No	String	Specifies the project ID.

Parameter	Mandatory	Type	Description
type	Yes	String	Specifies the type of the forwarding rule. Value options: • **HOST_NAME**: A domain name will be used for matching. • **PATH**: A URL will be used for matching. • **METHOD**: An HTTP request method will be used for matching. • **HEADER**: The request header will be used for matching. • **QUERY_STRING**: A query string will be used for matching. • **SOURCE_IP**: The source IP address will be used for matching. • **COOKIE**: The cookie will be used for matching. Note: If **type** is set to **HOST_NAME**, **PATH**, **METHOD**, or **SOURCE_IP**, only one forwarding rule can be created for each type. If **type** is set to **HEADER** and **QUERY_STRING**, multiple forwarding rules can be created for each type.
invert	No	Boolean	Specifies whether reverse matching is supported. Value range: **true** or **false** Default value: **false** This parameter is unsupported. Please do not use it.

Parameter	Mandatory	Type	Description
conditions	No	Array of **CreateRuleCondition** objects	Specifies the conditions contained in a forwarding rule. Note: • This parameter will take effect when **enhance_l7policy_enable** is set to **true**. • If **conditions** is specified, **key** and **value** will not take effect. • The keys in the list must be the same, whereas each value must be unique.

Table 5-612 CreateRuleCondition

Parameter	Mandatory	Type	Description
key	No	String	Specifies the key of match item. Note: • All keys in the conditions list in the same rule must be the same. • If **type** is set to **HOST_NAME**, **PATH**, **METHOD**, or **SOURCE_IP**, this parameter is an empty string. • If **type** is set to **HEADER**, **key** indicates the name of the HTTP header parameter, and **value** indicates the value of the request header parameter. The value can contain 1 to 40 characters, including letters, digits, hyphens (-), and underscores (_). • If **type** is set to **QUERY_STRING**, **key** indicates the name of the query parameter, and **value** indicates the value of the query parameter. The key is case sensitive and can contain 1 to 128 characters. Spaces, square brackets ([ ]), curly brackets ({ }), angle brackets (< >), backslashes (), double quotation marks (" "), pound signs (#), ampersands (&), vertical bars (|), percent signs (%), and tildes (~) are not supported.

Parameter	Mandatory	Type	Description
value	Yes	String	Specifies the value of the match item. Note: • The key of each condition in a forwarding policy must be the same. • The value of each condition in a forwarding policy must be unique. Value ranges: • If **type** is set to **HOST_NAME**, **key** is left blank, **value** indicates the domain name, which can contain 1 to 128 characters, including letters, digits, hyphens (-), periods (.), and asterisks (*), and must start with a letter, digit, or asterisk (*). If you want to use a wildcard domain name, enter an asterisk (*) as the leftmost label of the domain name. • If **type** is set to **PATH**, **key** is left blank, **value** indicates the request path, which can contain 1 to 128 characters. If **compare_type** is set to **STARTS_WITH** or **EQUAL_TO** for the forwarding rule, the value must start with a slash (/) and can contain only letters, digits, and special characters: _~';@^-%#&$.*+?,=!:|/()[]{} • If **type** is set to **HEADER**, **key** indicates the name of the HTTP header parameter and **value** indicates the value of the HTTP header parameter. The value can contain 1 to 128 characters. Asterisks (*) and question marks (?) are allowed, but spaces and double

Parameter	Mandatory	Type	Description
			quotation marks are not allowed. An asterisk can match zero or more characters, and a question mark can match 1 character. • If **type** is set to **QUERY_STRING**, **key** indicates the name of the query parameter and **value** indicates the value of the query parameter. The value is case sensitive and can contain 1 to 128 characters. Spaces, square brackets ([ ]), curly brackets ({ }), angle brackets (< >), backslashes (), double quotation marks (" "), pound signs (#), ampersands (&), vertical bars (|), percent signs (%), and tildes (~) are not supported. Asterisks (*) and question marks (?) are allowed. An asterisk can match zero or more characters, and a question mark can match 1 character. • If **type** is set to **METHOD**, **key** is left blank, **value** indicates the HTTP method. The value can be **GET**, **PUT**, **POST**, **DELETE**, **PATCH**, **HEAD**, or **OPTIONS**. • If **type** is set to **SOURCE_IP**, **key** is left blank, **value** indicates the source IP address of the request. The value is an IPv4 or IPv6 CIDR block, for example, 192.168.0.2/32 or 2049::49/64.

Response Parameters

Status code: 201

Table 5-613 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
rule	**L7Rule** object	Specifies the forwarding rule.

Table 5-614 L7Rule

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the forwarding rule. The default value is **true**. This parameter is unsupported. Please do not use it.
compare_type	String	Specifies how requests are matched with the domain name or URL. Value options: • If **type** is set to **HOST_NAME**, this parameter can only be set to **EQUAL_TO**. • If **type** is set to **PATH**, the value can be **REGEX**, **STARTS_WITH**, or **EQUAL_TO**.
key	String	Specifies the key of the match content. Note: This parameter will not take effect if **type** is set to **HOST_NAME** or **PATH**.
project_id	String	Specifies the project ID.

Parameter	Type	Description
type	String	Specifies the type of the forwarding rule. Value options: • **HOST_NAME**: A domain name will be used for matching. • **PATH**: A URL will be used for matching. • **METHOD**: An HTTP request method will be used for matching. • **HEADER**: The request header will be used for matching. • **QUERY_STRING**: A query string will be used for matching. • **SOURCE_IP**: The source IP address will be used for matching. • **COOKIE**: The cookie will be used for matching. Note: If **type** is set to **HOST_NAME**, **PATH**, **METHOD**, or **SOURCE_IP**, only one forwarding rule can be created for each type. If **type** is set to **HEADER** and **QUERY_STRING**, multiple forwarding rules can be created for each type.

Parameter	Type	Description
value	String	Specifies the value of the match item. Note: • This parameter will take effect only when **conditions** is left blank. • If **type** is set to **HOST_NAME**, the value can contain letters, digits, hyphens (-), and periods (.) and must start with a letter or digit. If you want to use a wildcard domain name, enter an asterisk (*) as the leftmost label of the domain name. • If **type** is set to **PATH** and **compare_type** to **STARTS_WITH** or **EQUAL_TO**, the value must start with a slash (/) and can contain only letters, digits, and special characters _~';@^-%#&$.*+?,=!:|\/()[]{} • If **type** is set to **METHOD**, **SOURCE_IP**, **HEADER**, or **QUERY_STRING**, this parameter will not take effect, and **condition_pair** will be used to specify the key and value.
provisioning_status	String	Specifies the provisioning status of the forwarding rule. The value can only be **ACTIVE** (default), **PENDING_CREATE**, or **ERROR**. This parameter is unsupported. Please do not use it.
invert	Boolean	Specifies whether reverse matching is supported. The value is fixed at **false**. This parameter can be updated but will not take effect.
id	String	Specifies the forwarding rule ID.

Parameter	Type	Description
conditions	Array of **RuleCondition** objects	Specifies the conditions contained in a forwarding rule. Note: • This parameter will take effect when **enhance_l7policy_enable** is set to **true**. • If **conditions** is specified, **key** and **value** will not take effect. • The keys in the list must be the same, whereas each value must be unique.
created_at	String	Specifies the time when the forwarding rule was added. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
updated_at	String	Specifies the time when the forwarding rule was updated. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.

Table 5-615 RuleCondition

Parameter	Type	Description
key	String	Specifies the key of match item. Note: • All keys in the conditions list in the same rule must be the same. • If **type** is set to **HOST_NAME**, **PATH**, **METHOD**, or **SOURCE_IP**, this parameter is an empty string. • If **type** is set to **HEADER**, **key** indicates the name of the HTTP header parameter, and **value** indicates the value of the request header parameter. The value can contain 1 to 40 characters, including letters, digits, hyphens (-), and underscores (_). • If **type** is set to **QUERY_STRING**, **key** indicates the name of the query parameter, and **value** indicates the value of the query parameter. The key is case sensitive and can contain 1 to 128 characters. Spaces, square brackets ([ ]), curly brackets ({ }), angle brackets (< >), backslashes (), double quotation marks (" "), pound signs (#), ampersands (&), vertical bars (|), percent signs (%), and tildes (~) are not supported.

Parameter	Type	Description
value	String	Specifies the value of the match item. Note: • The key of each condition in a forwarding policy must be the same. • The value of each condition in a forwarding policy must be unique. Value ranges: • If **type** is set to **HOST_NAME**, **key** is left blank, **value** indicates the domain name, which can contain 1 to 128 characters, including letters, digits, hyphens (-), periods (.), and asterisks (*), and must start with a letter, digit, or asterisk (*). If you want to use a wildcard domain name, enter an asterisk (*) as the leftmost label of the domain name. • If **type** is set to **PATH**, **key** is left blank, **value** indicates the request path, which can contain 1 to 128 characters. If **compare_type** is set to **STARTS_WITH** or **EQUAL_TO** for the forwarding rule, the value must start with a slash (/) and can contain only letters, digits, and special characters: _~';@^-%#&$.* +?,=!:|/()[]{} • If **type** is set to **HEADER**, **key** indicates the name of the HTTP header parameter and **value** indicates the value of the HTTP header parameter. The value can contain 1 to 128 characters. Asterisks (*) and question marks (?) are allowed, but spaces and double quotation marks are not allowed. An asterisk can match zero or more characters, and a question mark can match 1 character. • If **type** is set to **QUERY_STRING**, **key** indicates the name of the query parameter and **value** indicates the value of the query parameter. The value is case sensitive and can contain 1 to 128 characters. Spaces, square brackets ([ ]), curly brackets ({ }), angle

Parameter	Type	Description
		brackets (< >), backslashes (), double quotation marks (" "), pound signs (#), ampersands (&), vertical bars (|), percent signs (%), and tildes (~) are not supported. Asterisks (*) and question marks (?) are allowed. An asterisk can match zero or more characters, and a question mark can match 1 character. • If **type** is set to **METHOD**, **key** is left blank, **value** indicates the HTTP method. The value can be **GET**, **PUT**, **POST**, **DELETE**, **PATCH**, **HEAD**, or **OPTIONS**. • If **type** is set to **SOURCE_IP**, **key** is left blank, **value** indicates the source IP address of the request. The value is an IPv4 or IPv6 CIDR block, for example, 192.168.0.2/32 or 2049::49/64.

Example Requests

Creating a forwarding rule and setting **type** to *PATH*

```
POST https://{ELB_Endpoint}/v3/{99a3fff0d03c428eac3678da6a7d0f24}/elb/l7policies/cf4360fd-8631-41ff-a6f5-b72c35da74be/rules

{
  "rule" : {
    "compare_type" : "EQUAL_TO",
    "type" : "PATH",
    "value" : "/bbb.html"
  }
}
```

Example Responses

Status code: 201

Normal response to POST requests.

```
{
  "rule" : {
    "compare_type" : "EQUAL_TO",
    "provisioning_status" : "ACTIVE",
    "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
    "invert" : false,
    "admin_state_up" : true,
    "value" : "/bbb.html",
    "key" : null,
    "type" : "PATH",
    "id" : "84f4fcae-9c15-4e19-a99f-72c0b08fd3d7"
  },
```



```
  "request_id" : "3639f1b7-f04b-496e-9218-ec5a9e493f69"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Creating a forwarding rule and setting **type** to *PATH*

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class CreateL7RuleSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateL7RuleRequest request = new CreateL7RuleRequest();
        request.withL7policyId("{l7policy_id}");
        CreateL7RuleRequestBody body = new CreateL7RuleRequestBody();
        CreateRuleOption rulebody = new CreateRuleOption();
        rulebody.withCompareType("EQUAL_TO")
            .withValue("/bbb.html")
            .withType("PATH");
        body.withRule(rulebody);
        request.withBody(body);
        try {
            CreateL7RuleResponse response = client.createL7Rule(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

Creating a forwarding rule and setting **type** to *PATH*

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateL7RuleRequest()
        request.l7policy_id = "{l7policy_id}"
        rulebody = CreateRuleOption(
            compare_type="EQUAL_TO",
            value="/bbb.html",
            type="PATH"
        )
        request.body = CreateL7RuleRequestBody(
            rule=rulebody
        )
        response = client.create_l7_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

Creating a forwarding rule and setting **type** to *PATH*

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
      elb.ElbClientBuilder().
         WithRegion(region.ValueOf("<YOUR REGION>")).
         WithCredential(auth).
         Build())

   request := &model.CreateL7RuleRequest{}
   request.L7policyId = "{l7policy_id}"
   rulebody := &model.CreateRuleOption{
      CompareType: "EQUAL_TO",
      Value: "/bbb.html",
      Type: "PATH",
   }
   request.Body = &model.CreateL7RuleRequestBody{
      Rule: rulebody,
   }
   response, err := client.CreateL7Rule(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 POST requests.

Error Codes

See **Error Codes**.

5.15.2 Querying Forwarding Rules

Function

This API is used to query all forwarding rules.

Constraints

This API has the following constraints:

- Parameters **marker**, **limit**, and **page_reverse** are used for pagination query.
- Parameters **marker** and **page_reverse** take effect only when they are used together with parameter **limit**.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/l7policies/{l7policy_id}/rules

Table 5-616 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
l7policy_id	Yes	String	Specifies the forwarding policy ID.

Table 5-617 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Specifies the number of records on each page. Value range: 0–2000 Default value: 2000
marker	No	String	Specifies the ID of the last record on the previous page. Note: • This parameter must be used together with **limit**. • If this parameter is not specified, the first page will be queried. • This parameter cannot be left blank or set to an invalid ID.

Parameter	Mandatory	Type	Description
page_reverse	No	Boolean	Specifies whether to use reverse query. Value options: • **true**: Query the previous page. • **false** (default): Query the next page. Note: • This parameter must be used together with **limit**. • If **page_reverse** is set to **true** and you want to query the previous page, set the value of **marker** to the value of **previous_marker**.
id	No	Array of strings	Specifies the forwarding rule ID. Multiple IDs can be queried in the format of *id=xxx&id=xxx*.
compare_type	No	Array of strings	Specifies how requests are matched with the domain names or URL. Value options: • **EQUAL_TO**: exact match. • **REGEX**: regular expression match • **STARTS_WITH**: prefix match Multiple values can be queried in the format of *compare_type=xxx&compare_type=xxx*.
provisioning_status	No	Array of strings	Specifies the provisioning status of the forwarding rule. The value can only be **ACTIVE**, indicating that the forwarding rule is provisioned successfully. Multiple provisioning statuses can be queried in the format of *provisioning_status=xxx&provisioning_status=xxx*.

Parameter	Mandatory	Type	Description
invert	No	Boolean	Specifies whether reverse matching is supported. The value is fixed at **false**. This parameter can be updated but remains invalid.
admin_state_up	No	Boolean	Specifies the administrative status of the forwarding rule. This parameter is unsupported. Please do not use it.
value	No	Array of strings	Specifies the value of the match content. Multiple values can be queried in the format of *value=xxx&value=xxx*.
key	No	Array of strings	Specifies the key of the match content that is used to identify the forwarding rule. Multiple keys can be queried in the format of *key=xxx&key=xxx*. This parameter is unsupported. Please do not use it.
type	No	Array of strings	Specifies the match type. The value can be **HOST_NAME** or **PATH**. The type of forwarding rules for the same forwarding policy cannot be the same. Multiple types can be queried in the format of *type=xxx&type=xxx*.

Parameter	Mandatory	Type	Description
enterprise_project_id	No	Array of strings	Specifies the ID of the enterprise project. • If **enterprise_project_id** is not specified, resources in all enterprise projects are queried by default. Fine-grained authorization is performed. The **elb:l7rules:list** permission must be assigned to the user group. • If **enterprise_project_id** is specified, the value can be a specific enterprise project ID or **all_granted_eps**. If the value is a specific enterprise project ID, only resources in the enterprise project are queried. If the value is **all_granted_eps**, resources in the enterprise projects with the **elb:l7rules:list** permission are queried. Multiple values can be queried in the format of *enterprise_project_id=xxx&enterprise_project_id=xxx*.

Request Parameters

Table 5-618 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-619 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
page_info	**PageInfo** object	Shows pagination information.
rules	Array of **L7Rule** objects	Lists the forwarding rules.

Table 5-620 PageInfo

Parameter	Type	Description
previous_marker	String	Specifies the ID of the first record in the pagination query result. When **page_reverse** is set to **true**, this parameter is used together to query resources on the previous page.
next_marker	String	Specifies the ID of the last record in the pagination query result.
current_count	Integer	Specifies the number of records.

Table 5-621 L7Rule

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the forwarding rule. The default value is **true**. This parameter is unsupported. Please do not use it.
compare_type	String	Specifies how requests are matched with the domain name or URL. Value options: • If **type** is set to **HOST_NAME**, this parameter can only be set to **EQUAL_TO**. • If **type** is set to **PATH**, the value can be **REGEX**, **STARTS_WITH**, or **EQUAL_TO**.

Parameter	Type	Description
key	String	Specifies the key of the match content. Note: This parameter will not take effect if **type** is set to **HOST_NAME** or **PATH**.
project_id	String	Specifies the project ID.
type	String	Specifies the type of the forwarding rule. Value options: • **HOST_NAME**: A domain name will be used for matching. • **PATH**: A URL will be used for matching. • **METHOD**: An HTTP request method will be used for matching. • **HEADER**: The request header will be used for matching. • **QUERY_STRING**: A query string will be used for matching. • **SOURCE_IP**: The source IP address will be used for matching. • **COOKIE**: The cookie will be used for matching. Note: If **type** is set to **HOST_NAME**, **PATH**, **METHOD**, or **SOURCE_IP**, only one forwarding rule can be created for each type. If **type** is set to **HEADER** and **QUERY_STRING**, multiple forwarding rules can be created for each type.

Parameter	Type	Description
value	String	Specifies the value of the match item. Note: • This parameter will take effect only when **conditions** is left blank. • If **type** is set to **HOST_NAME**, the value can contain letters, digits, hyphens (-), and periods (.) and must start with a letter or digit. If you want to use a wildcard domain name, enter an asterisk (*) as the leftmost label of the domain name. • If **type** is set to **PATH** and **compare_type** to **STARTS_WITH** or **EQUAL_TO**, the value must start with a slash (/) and can contain only letters, digits, and special characters _~';@^-%#&$.*+?,=!:|\/()[]{} • If **type** is set to **METHOD**, **SOURCE_IP**, **HEADER**, or **QUERY_STRING**, this parameter will not take effect, and **condition_pair** will be used to specify the key and value.
provisioning_status	String	Specifies the provisioning status of the forwarding rule. The value can only be **ACTIVE** (default), **PENDING_CREATE**, or **ERROR**. This parameter is unsupported. Please do not use it.
invert	Boolean	Specifies whether reverse matching is supported. The value is fixed at **false**. This parameter can be updated but will not take effect.
id	String	Specifies the forwarding rule ID.

Parameter	Type	Description
conditions	Array of **RuleCondition** objects	Specifies the conditions contained in a forwarding rule. Note: • This parameter will take effect when **enhance_l7policy_enable** is set to **true**. • If **conditions** is specified, **key** and **value** will not take effect. • The keys in the list must be the same, whereas each value must be unique.
created_at	String	Specifies the time when the forwarding rule was added. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
updated_at	String	Specifies the time when the forwarding rule was updated. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.

Table 5-622 RuleCondition

Parameter	Type	Description
key	String	Specifies the key of match item. Note: • All keys in the conditions list in the same rule must be the same. • If **type** is set to **HOST_NAME**, **PATH**, **METHOD**, or **SOURCE_IP**, this parameter is an empty string. • If **type** is set to **HEADER**, **key** indicates the name of the HTTP header parameter, and **value** indicates the value of the request header parameter. The value can contain 1 to 40 characters, including letters, digits, hyphens (-), and underscores (_). • If **type** is set to **QUERY_STRING**, **key** indicates the name of the query parameter, and **value** indicates the value of the query parameter. The key is case sensitive and can contain 1 to 128 characters. Spaces, square brackets ([ ]), curly brackets ({ }), angle brackets (< >), backslashes (), double quotation marks (" "), pound signs (#), ampersands (&), vertical bars (|), percent signs (%), and tildes (~) are not supported.

Parameter	Type	Description
value	String	Specifies the value of the match item. Note: • The key of each condition in a forwarding policy must be the same. • The value of each condition in a forwarding policy must be unique. Value ranges: • If **type** is set to **HOST_NAME**, **key** is left blank, **value** indicates the domain name, which can contain 1 to 128 characters, including letters, digits, hyphens (-), periods (.), and asterisks (*), and must start with a letter, digit, or asterisk (*). If you want to use a wildcard domain name, enter an asterisk (*) as the leftmost label of the domain name. • If **type** is set to **PATH**, **key** is left blank, **value** indicates the request path, which can contain 1 to 128 characters. If **compare_type** is set to **STARTS_WITH** or **EQUAL_TO** for the forwarding rule, the value must start with a slash (/) and can contain only letters, digits, and special characters: _~';@^-%#&$.* +?,=!:|/()[]{} • If **type** is set to **HEADER**, **key** indicates the name of the HTTP header parameter and **value** indicates the value of the HTTP header parameter. The value can contain 1 to 128 characters. Asterisks (*) and question marks (?) are allowed, but spaces and double quotation marks are not allowed. An asterisk can match zero or more characters, and a question mark can match 1 character. • If **type** is set to **QUERY_STRING**, **key** indicates the name of the query parameter and **value** indicates the value of the query parameter. The value is case sensitive and can contain 1 to 128 characters. Spaces, square brackets ([ ]), curly brackets ({ }), angle

Parameter	Type	Description
		brackets (< >), backslashes (), double quotation marks (" "), pound signs (#), ampersands (&), vertical bars (|), percent signs (%), and tildes (~) are not supported. Asterisks (*) and question marks (?) are allowed. An asterisk can match zero or more characters, and a question mark can match 1 character. • If **type** is set to **METHOD**, **key** is left blank, **value** indicates the HTTP method. The value can be **GET**, **PUT**, **POST**, **DELETE**, **PATCH**, **HEAD**, or **OPTIONS**. • If **type** is set to **SOURCE_IP**, **key** is left blank, **value** indicates the source IP address of the request. The value is an IPv4 or IPv6 CIDR block, for example, 192.168.0.2/32 or 2049::49/64.

Example Requests

Querying forwarding rules

```
GET https://{ELB_Endpoint}/v3/{99a3fff0d03c428eac3678da6a7d0f24}/elb/l7policies/cf4360fd-8631-41ff-a6f5-b72c35da74be/rules
```

Example Responses

Status code: 200

Successful request.

```
{
  "rules" : [ {
    "compare_type" : "STARTS_WITH",
    "provisioning_status" : "ACTIVE",
    "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
    "invert" : false,
    "admin_state_up" : true,
    "value" : "/ccc.html",
    "key" : null,
    "type" : "PATH",
    "id" : "84f4fcae-9c15-4e19-a99f-72c0b08fd3d7"
  } ],
  "page_info" : {
    "previous_marker" : "84f4fcae-9c15-4e19-a99f-72c0b08fd3d7",
    "current_count" : 1
  },
  "request_id" : "ae4dbd7d-9271-4040-98b6-3bfe45bb15ee"
}
```


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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ListL7RulesSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ListL7RulesRequest request = new ListL7RulesRequest();
        request.withL7policyId("{l7policy_id}");
        try {
            ListL7RulesResponse response = client.listL7Rules(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListL7RulesRequest()
        request.l7policy_id = "{l7policy_id}"
        response = client.list_l7_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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListL7RulesRequest{}
    request.L7policyId = "{l7policy_id}"
    response, err := client.ListL7Rules(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	Successful request.

Error Codes

See **Error Codes**.

5.15.3 Viewing the Details of a Forwarding Rule

Function

This API is used to view the details of a forwarding rule.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/l7policies/{l7policy_id}/rules/{l7rule_id}

Table 5-623 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
l7policy_id	Yes	String	Specifies the forwarding policy.
l7rule_id	Yes	String	Specifies the forwarding rule.

Request Parameters

Table 5-624 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-625 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
rule	**L7Rule** object	Specifies the forwarding rule.

Table 5-626 L7Rule

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the forwarding rule. The default value is **true**. This parameter is unsupported. Please do not use it.
compare_type	String	Specifies how requests are matched with the domain name or URL. Value options: • If **type** is set to **HOST_NAME**, this parameter can only be set to **EQUAL_TO**. • If **type** is set to **PATH**, the value can be **REGEX**, **STARTS_WITH**, or **EQUAL_TO**.
key	String	Specifies the key of the match content. Note: This parameter will not take effect if **type** is set to **HOST_NAME** or **PATH**.
project_id	String	Specifies the project ID.

Parameter	Type	Description
type	String	Specifies the type of the forwarding rule. Value options: • **HOST_NAME**: A domain name will be used for matching. • **PATH**: A URL will be used for matching. • **METHOD**: An HTTP request method will be used for matching. • **HEADER**: The request header will be used for matching. • **QUERY_STRING**: A query string will be used for matching. • **SOURCE_IP**: The source IP address will be used for matching. • **COOKIE**: The cookie will be used for matching. Note: If **type** is set to **HOST_NAME**, **PATH**, **METHOD**, or **SOURCE_IP**, only one forwarding rule can be created for each type. If **type** is set to **HEADER** and **QUERY_STRING**, multiple forwarding rules can be created for each type.

Parameter	Type	Description
value	String	Specifies the value of the match item. Note: • This parameter will take effect only when **conditions** is left blank. • If **type** is set to **HOST_NAME**, the value can contain letters, digits, hyphens (-), and periods (.) and must start with a letter or digit. If you want to use a wildcard domain name, enter an asterisk (*) as the leftmost label of the domain name. • If **type** is set to **PATH** and **compare_type** to **STARTS_WITH** or **EQUAL_TO**, the value must start with a slash (/) and can contain only letters, digits, and special characters _~';@^-%#&$.*+?,=!:|\/()[]{} • If **type** is set to **METHOD**, **SOURCE_IP**, **HEADER**, or **QUERY_STRING**, this parameter will not take effect, and **condition_pair** will be used to specify the key and value.
provisioning_status	String	Specifies the provisioning status of the forwarding rule. The value can only be **ACTIVE** (default), **PENDING_CREATE**, or **ERROR**. This parameter is unsupported. Please do not use it.
invert	Boolean	Specifies whether reverse matching is supported. The value is fixed at **false**. This parameter can be updated but will not take effect.
id	String	Specifies the forwarding rule ID.

Parameter	Type	Description
conditions	Array of **RuleCondition** objects	Specifies the conditions contained in a forwarding rule. Note: • This parameter will take effect when **enhance_l7policy_enable** is set to **true**. • If **conditions** is specified, **key** and **value** will not take effect. • The keys in the list must be the same, whereas each value must be unique.
created_at	String	Specifies the time when the forwarding rule was added. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
updated_at	String	Specifies the time when the forwarding rule was updated. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.

Table 5-627 RuleCondition

Parameter	Type	Description
key	String	Specifies the key of match item. Note: • All keys in the conditions list in the same rule must be the same. • If **type** is set to **HOST_NAME**, **PATH**, **METHOD**, or **SOURCE_IP**, this parameter is an empty string. • If **type** is set to **HEADER**, **key** indicates the name of the HTTP header parameter, and **value** indicates the value of the request header parameter. The value can contain 1 to 40 characters, including letters, digits, hyphens (-), and underscores (_). • If **type** is set to **QUERY_STRING**, **key** indicates the name of the query parameter, and **value** indicates the value of the query parameter. The key is case sensitive and can contain 1 to 128 characters. Spaces, square brackets ([ ]), curly brackets ({ }), angle brackets (< >), backslashes (), double quotation marks (" "), pound signs (#), ampersands (&), vertical bars (|), percent signs (%), and tildes (~) are not supported.

Parameter	Type	Description
value	String	Specifies the value of the match item. Note: • The key of each condition in a forwarding policy must be the same. • The value of each condition in a forwarding policy must be unique. Value ranges: • If **type** is set to **HOST_NAME**, **key** is left blank, **value** indicates the domain name, which can contain 1 to 128 characters, including letters, digits, hyphens (-), periods (.), and asterisks (*), and must start with a letter, digit, or asterisk (*). If you want to use a wildcard domain name, enter an asterisk (*) as the leftmost label of the domain name. • If **type** is set to **PATH**, **key** is left blank, **value** indicates the request path, which can contain 1 to 128 characters. If **compare_type** is set to **STARTS_WITH** or **EQUAL_TO** for the forwarding rule, the value must start with a slash (/) and can contain only letters, digits, and special characters: _~';@^-%#&$.* +?,=!:|/()[]{} • If **type** is set to **HEADER**, **key** indicates the name of the HTTP header parameter and **value** indicates the value of the HTTP header parameter. The value can contain 1 to 128 characters. Asterisks (*) and question marks (?) are allowed, but spaces and double quotation marks are not allowed. An asterisk can match zero or more characters, and a question mark can match 1 character. • If **type** is set to **QUERY_STRING**, **key** indicates the name of the query parameter and **value** indicates the value of the query parameter. The value is case sensitive and can contain 1 to 128 characters. Spaces, square brackets ([ ]), curly brackets ({ }), angle

Parameter	Type	Description
		brackets (< >), backslashes (), double quotation marks (" "), pound signs (#), ampersands (&), vertical bars (|), percent signs (%), and tildes (~) are not supported. Asterisks (*) and question marks (?) are allowed. An asterisk can match zero or more characters, and a question mark can match 1 character. • If **type** is set to **METHOD**, **key** is left blank, **value** indicates the HTTP method. The value can be **GET**, **PUT**, **POST**, **DELETE**, **PATCH**, **HEAD**, or **OPTIONS**. • If **type** is set to **SOURCE_IP**, **key** is left blank, **value** indicates the source IP address of the request. The value is an IPv4 or IPv6 CIDR block, for example, 192.168.0.2/32 or 2049::49/64.

Example Requests

Querying the details of a given forwarding rule

```
GET https://{ELB_Endpoint}/v3/{99a3fff0d03c428eac3678da6a7d0f24}/elb/l7policies/cf4360fd-8631-41ff-a6f5-b72c35da74be/rules/84f4fcae-9c15-4e19-a99f-72c0b08fd3d7
```

Example Responses

Status code: 200

OK

```
{
  "rule" : {
    "compare_type" : "STARTS_WITH",
    "provisioning_status" : "ACTIVE",
    "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
    "invert" : false,
    "admin_state_up" : true,
    "value" : "/ccc.html",
    "key" : null,
    "type" : "PATH",
    "id" : "84f4fcae-9c15-4e19-a99f-72c0b08fd3d7"
  },
  "request_id" : "0d799435-259e-459f-b2bc-0beee06f6a77"
}
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ShowL7RuleSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowL7RuleRequest request = new ShowL7RuleRequest();
        request.withL7policyId("{l7policy_id}");
        request.withL7ruleId("{l7rule_id}");
        try {
            ShowL7RuleResponse response = client.showL7Rule(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowL7RuleRequest()
        request.l7policy_id = "{l7policy_id}"
        request.l7rule_id = "{l7rule_id}"
        response = client.show_l7_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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowL7RuleRequest{}
    request.L7policyId = "{l7policy_id}"
    request.L7ruleId = "{l7rule_id}"
    response, err := client.ShowL7Rule(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**.

5.15.4 Updating a Forwarding Rule

Function

This API is used to update a forwarding rule.

Calling Method

For details, see **Calling APIs**.

URI

PUT /v3/{project_id}/elb/l7policies/{l7policy_id}/rules/{l7rule_id}

Table 5-628 Path Parameters

Parameter	Mandatory	Type	Description
l7policy_id	Yes	String	Specifies the forwarding policy ID.
l7rule_id	Yes	String	Specifies the forwarding rule ID.
project_id	Yes	String	Specifies the project ID.

Request Parameters

Table 5-629 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Table 5-630 Request body parameters

Parameter	Mandatory	Type	Description
rule	Yes	**UpdateL7RuleOption** object	Specifies the forwarding rule.

Table 5-631 UpdateL7RuleOption

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Specifies the administrative status of the forwarding rule. The value can only be **true**.

Parameter	Mandatory	Type	Description
compare_type	No	String	Specifies how requests are matched with the forwarding rule. Value options: • **EQUAL_TO**: exact match. • **REGEX**: regular expression match • **STARTS_WITH**: prefix match Note: • If **type** is set to **HOST_NAME**, the value can only be **EQUAL_TO**, and asterisks (*) can be used as wildcard characters. • If **type** is set to **PATH**, the value can be **REGEX**, **STARTS_WITH**, or **EQUAL_TO**. • If **type** is set to **METHOD** or **SOURCE_IP**, the value can only be **EQUAL_TO**. • If **type** is set to **HEADER** or **QUERY_STRING**, the value can only be **EQUAL_TO**, asterisks (*) and question marks (?) can be used as wildcard characters.
invert	No	Boolean	Specifies whether reverse matching is supported. The value can be **true** or **false**. This parameter is unsupported. Please do not use it.
key	No	String	Specifies the key of the match item. For example, if an HTTP header is used for matching, **key** is the name of the HTTP header parameter. This parameter is unsupported. Please do not use it.

Parameter	Mandatory	Type	Description
value	No	String	Specifies the value of the match item. For example, if a domain name is used for matching, **value** is the domain name. Note: • This parameter will take effect only when **conditions** is left blank. • If **type** is set to **HOST_NAME**, the value can contain letters, digits, hyphens (-), and periods (.) and must start with a letter or digit. If you want to use a wildcard domain name, enter an asterisk (*) as the leftmost label of the domain name. • If **type** is set to **PATH** and **compare_type** to **STARTS_WITH** or **EQUAL_TO**, the value must start with a slash (/) and can contain only letters, digits, and special characters _~';@^-%#&$.* +?,=!:|\/()[]{} • If **type** is set to **METHOD**, **SOURCE_IP**, **HEADER**, or **QUERY_STRING**, this parameter will not take effect, and **conditions** will be used to specify the key and value.

Parameter	Mandatory	Type	Description
conditions	No	Array of **UpdateRuleCondition** objects	Specifies the conditions contained in a forwarding rule. Note: • This parameter will take effect when **enhance_l7policy_enable** is set to **true**. • If **conditions** is specified, **key** and **value** will not take effect. • The keys in the list must be the same, whereas each value must be unique.

Table 5-632 UpdateRuleCondition

Parameter	Mandatory	Type	Description
key	No	String	Specifies the key of match item. Note: • All keys in the conditions list in the same rule must be the same. • If **type** is set to **HOST_NAME**, **PATH**, **METHOD**, or **SOURCE_IP**, this parameter is an empty string. • If **type** is set to **HEADER**, **key** indicates the name of the HTTP header parameter, and **value** indicates the value of the request header parameter. The value can contain 1 to 40 characters, including letters, digits, hyphens (-), and underscores (_). • If **type** is set to **QUERY_STRING**, **key** indicates the name of the query parameter, and **value** indicates the value of the query parameter. The key is case sensitive and can contain 1 to 128 characters. Spaces, square brackets ([ ]), curly brackets ({ }), angle brackets (< >), backslashes (), double quotation marks (" "), pound signs (#), ampersands (&), vertical bars (|), percent signs (%), and tildes (~) are not supported.

Parameter	Mandatory	Type	Description
value	No	String	Specifies the value of the match item. Note: • The key of each condition in a forwarding policy must be the same. • The value of each condition in a forwarding policy must be unique. Value ranges: • If **type** is set to **HOST_NAME**, **key** is left blank, **value** indicates the domain name, which can contain 1 to 128 characters, including letters, digits, hyphens (-), periods (.), and asterisks (*), and must start with a letter, digit, or asterisk (*). If you want to use a wildcard domain name, enter an asterisk (*) as the leftmost label of the domain name. • If **type** is set to **PATH**, **key** is left blank, **value** indicates the request path, which can contain 1 to 128 characters. If **compare_type** is set to **STARTS_WITH** or **EQUAL_TO** for the forwarding rule, the value must start with a slash (/) and can contain only letters, digits, and special characters: _~';@^-%#&$.*+?,=!:|/()[]{} • If **type** is set to **HEADER**, **key** indicates the name of the HTTP header parameter and **value** indicates the value of the HTTP header parameter. The value can contain 1 to 128 characters. Asterisks (*) and question marks (?) are allowed, but spaces and double

Parameter	Mandatory	Type	Description
			quotation marks are not allowed. An asterisk can match zero or more characters, and a question mark can match 1 character. • If **type** is set to **QUERY_STRING**, **key** indicates the name of the query parameter and **value** indicates the value of the query parameter. The value is case sensitive and can contain 1 to 128 characters. Spaces, square brackets ([ ]), curly brackets ({ }), angle brackets (< >), backslashes (), double quotation marks (" "), pound signs (#), ampersands (&), vertical bars (|), percent signs (%), and tildes (~) are not supported. Asterisks (*) and question marks (?) are allowed. An asterisk can match zero or more characters, and a question mark can match 1 character. • If **type** is set to **METHOD**, **key** is left blank, **value** indicates the HTTP method. The value can be **GET**, **PUT**, **POST**, **DELETE**, **PATCH**, **HEAD**, or **OPTIONS**. • If **type** is set to **SOURCE_IP**, **key** is left blank, **value** indicates the source IP address of the request. The value is an IPv4 or IPv6 CIDR block, for example, 192.168.0.2/32 or 2049::49/64.

Response Parameters

Status code: 200

Table 5-633 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
rule	**L7Rule** object	Specifies the forwarding rule.

Table 5-634 L7Rule

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the forwarding rule. The default value is **true**. This parameter is unsupported. Please do not use it.
compare_type	String	Specifies how requests are matched with the domain name or URL. Value options: • If **type** is set to **HOST_NAME**, this parameter can only be set to **EQUAL_TO**. • If **type** is set to **PATH**, the value can be **REGEX**, **STARTS_WITH**, or **EQUAL_TO**.
key	String	Specifies the key of the match content. Note: This parameter will not take effect if **type** is set to **HOST_NAME** or **PATH**.
project_id	String	Specifies the project ID.

Parameter	Type	Description
type	String	Specifies the type of the forwarding rule. Value options: • **HOST_NAME**: A domain name will be used for matching. • **PATH**: A URL will be used for matching. • **METHOD**: An HTTP request method will be used for matching. • **HEADER**: The request header will be used for matching. • **QUERY_STRING**: A query string will be used for matching. • **SOURCE_IP**: The source IP address will be used for matching. • **COOKIE**: The cookie will be used for matching. Note: If **type** is set to **HOST_NAME**, **PATH**, **METHOD**, or **SOURCE_IP**, only one forwarding rule can be created for each type. If **type** is set to **HEADER** and **QUERY_STRING**, multiple forwarding rules can be created for each type.

Parameter	Type	Description
value	String	Specifies the value of the match item. Note: • This parameter will take effect only when **conditions** is left blank. • If **type** is set to **HOST_NAME**, the value can contain letters, digits, hyphens (-), and periods (.) and must start with a letter or digit. If you want to use a wildcard domain name, enter an asterisk (*) as the leftmost label of the domain name. • If **type** is set to **PATH** and **compare_type** to **STARTS_WITH** or **EQUAL_TO**, the value must start with a slash (/) and can contain only letters, digits, and special characters _~';@^-%#&$.*+?,=!:|\/()[]{} • If **type** is set to **METHOD**, **SOURCE_IP**, **HEADER**, or **QUERY_STRING**, this parameter will not take effect, and **condition_pair** will be used to specify the key and value.
provisioning_status	String	Specifies the provisioning status of the forwarding rule. The value can only be **ACTIVE** (default), **PENDING_CREATE**, or **ERROR**. This parameter is unsupported. Please do not use it.
invert	Boolean	Specifies whether reverse matching is supported. The value is fixed at **false**. This parameter can be updated but will not take effect.
id	String	Specifies the forwarding rule ID.

Parameter	Type	Description
conditions	Array of **RuleCondition** objects	Specifies the conditions contained in a forwarding rule. Note: • This parameter will take effect when **enhance_l7policy_enable** is set to **true**. • If **conditions** is specified, **key** and **value** will not take effect. • The keys in the list must be the same, whereas each value must be unique.
created_at	String	Specifies the time when the forwarding rule was added. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
updated_at	String	Specifies the time when the forwarding rule was updated. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.

Table 5-635 RuleCondition

Parameter	Type	Description
key	String	Specifies the key of match item. Note: • All keys in the conditions list in the same rule must be the same. • If **type** is set to **HOST_NAME**, **PATH**, **METHOD**, or **SOURCE_IP**, this parameter is an empty string. • If **type** is set to **HEADER**, **key** indicates the name of the HTTP header parameter, and **value** indicates the value of the request header parameter. The value can contain 1 to 40 characters, including letters, digits, hyphens (-), and underscores (_). • If **type** is set to **QUERY_STRING**, **key** indicates the name of the query parameter, and **value** indicates the value of the query parameter. The key is case sensitive and can contain 1 to 128 characters. Spaces, square brackets ([ ]), curly brackets ({ }), angle brackets (< >), backslashes (), double quotation marks (" "), pound signs (#), ampersands (&), vertical bars (|), percent signs (%), and tildes (~) are not supported.

Parameter	Type	Description
value	String	Specifies the value of the match item. Note: • The key of each condition in a forwarding policy must be the same. • The value of each condition in a forwarding policy must be unique. Value ranges: • If **type** is set to **HOST_NAME**, **key** is left blank, **value** indicates the domain name, which can contain 1 to 128 characters, including letters, digits, hyphens (-), periods (.), and asterisks (*), and must start with a letter, digit, or asterisk (*). If you want to use a wildcard domain name, enter an asterisk (*) as the leftmost label of the domain name. • If **type** is set to **PATH**, **key** is left blank, **value** indicates the request path, which can contain 1 to 128 characters. If **compare_type** is set to **STARTS_WITH** or **EQUAL_TO** for the forwarding rule, the value must start with a slash (/) and can contain only letters, digits, and special characters: _~';@^-%#&$.* +?,=!:|/()[]{} • If **type** is set to **HEADER**, **key** indicates the name of the HTTP header parameter and **value** indicates the value of the HTTP header parameter. The value can contain 1 to 128 characters. Asterisks (*) and question marks (?) are allowed, but spaces and double quotation marks are not allowed. An asterisk can match zero or more characters, and a question mark can match 1 character. • If **type** is set to **QUERY_STRING**, **key** indicates the name of the query parameter and **value** indicates the value of the query parameter. The value is case sensitive and can contain 1 to 128 characters. Spaces, square brackets ([ ]), curly brackets ({ }), angle

Parameter	Type	Description
		brackets (< >), backslashes (), double quotation marks (" "), pound signs (#), ampersands (&), vertical bars (|), percent signs (%), and tildes (~) are not supported. Asterisks (*) and question marks (?) are allowed. An asterisk can match zero or more characters, and a question mark can match 1 character. • If **type** is set to **METHOD**, **key** is left blank, **value** indicates the HTTP method. The value can be **GET**, **PUT**, **POST**, **DELETE**, **PATCH**, **HEAD**, or **OPTIONS**. • If **type** is set to **SOURCE_IP**, **key** is left blank, **value** indicates the source IP address of the request. The value is an IPv4 or IPv6 CIDR block, for example, 192.168.0.2/32 or 2049::49/64.

Example Requests

Modifying a forwarding rule

```
PUT https://{ELB_Endpoint}/v3/{99a3fff0d03c428eac3678da6a7d0f24}/elb/l7policies/cf4360fd-8631-41ff-a6f5-b72c35da74be/rules/84f4fcae-9c15-4e19-a99f-72c0b08fd3d7

{
  "rule" : {
    "compare_type" : "STARTS_WITH",
    "value" : "/ccc.html"
  }
}
```

Example Responses

Status code: 200

Successful request.

```
{
  "rule" : {
    "compare_type" : "STARTS_WITH",
    "provisioning_status" : "ACTIVE",
    "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
    "invert" : false,
    "admin_state_up" : true,
    "value" : "/ccc.html",
    "key" : null,
    "type" : "PATH",
    "id" : "84f4fcae-9c15-4e19-a99f-72c0b08fd3d7"
  },
```



```
  "request_id" : "133096f9-e754-430d-a2c2-e61fe1190aa8"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Modifying a forwarding rule

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class UpdateL7RuleSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdateL7RuleRequest request = new UpdateL7RuleRequest();
        request.withL7policyId("{l7policy_id}");
        request.withL7ruleId("{l7rule_id}");
        UpdateL7RuleRequestBody body = new UpdateL7RuleRequestBody();
        UpdateL7RuleOption rulebody = new UpdateL7RuleOption();
        rulebody.withCompareType("STARTS_WITH")
            .withValue("/ccc.html");
        body.withRule(rulebody);
        request.withBody(body);
        try {
            UpdateL7RuleResponse response = client.updateL7Rule(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

Modifying a forwarding rule

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdateL7RuleRequest()
        request.l7policy_id = "{l7policy_id}"
        request.l7rule_id = "{l7rule_id}"
        rulebody = UpdateL7RuleOption(
            compare_type="STARTS_WITH",
            value="/ccc.html"
        )
        request.body = UpdateL7RuleRequestBody(
            rule=rulebody
        )
        response = client.update_l7_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

Modifying a forwarding rule

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdateL7RuleRequest{}
    request.L7policyId = "{l7policy_id}"
    request.L7ruleId = "{l7rule_id}"
    compareTypeRule:= "STARTS_WITH"
    valueRule:= "/ccc.html"
    rulebody := &model.UpdateL7RuleOption{
        CompareType: &compareTypeRule,
        Value: &valueRule,
    }
    request.Body = &model.UpdateL7RuleRequestBody{
        Rule: rulebody,
    }
    response, err := client.UpdateL7Rule(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	Successful request.

Error Codes

See **Error Codes**.

5.15.5 Deleting a Forwarding Rule

Function

This API is used to delete a forwarding rule.

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v3/{project_id}/elb/l7policies/{l7policy_id}/rules/{l7rule_id}

Table 5-636 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
l7policy_id	Yes	String	Specifies the forwarding policy ID.
l7rule_id	Yes	String	Specifies the forwarding rule ID.

Request Parameters

Table 5-637 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

None

Example Requests

Deleting a forwarding rule

```
DELETE https://{ELB_Endpoint}/v3/{99a3fff0d03c428eac3678da6a7d0f24}/elb/l7policies/cf4360fd-8631-41ff-a6f5-b72c35da74be/rules/84f4fcae-9c15-4e19-a99f-72c0b08fd3d7
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class DeleteL7RuleSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteL7RuleRequest request = new DeleteL7RuleRequest();
        request.withL7policyId("{l7policy_id}");
        request.withL7ruleId("{l7rule_id}");
        try {
            DeleteL7RuleResponse response = client.deleteL7Rule(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteL7RuleRequest()
        request.l7policy_id = "{l7policy_id}"
        request.l7rule_id = "{l7rule_id}"
        response = client.delete_l7_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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteL7RuleRequest{}
    request.L7policyId = "{l7policy_id}"
    request.L7ruleId = "{l7rule_id}"
    response, err := client.DeleteL7Rule(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	Successful request.

Error Codes

See **Error Codes**.

5.16 Active/Standby Backend Server Group

5.16.1 Creating an Active/Standby Backend Server Group

Function

This API is used to create an active/standby backend server group.

Constraints

Note the following when you create a backend server group:

- If **session-persistence** is specified, **cookie_name** is available only when **type** is set to **APP_COOKIE**.
- If **listener_id** is specified, the listener must have no backend server group associated.

Calling Method

For details, see **Calling APIs**.

URI

POST /v3/{project_id}/elb/master-slave-pools

Table 5-638 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Request Parameters

Table 5-639 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Table 5-640 Request body parameters

Parameter	Mandatory	Type	Description
pool	Yes	**CreateMasterSlavePoolOption** object	Specifies the request body for creating a backend server group.

Table 5-641 CreateMasterSlavePoolOption

Parameter	Mandatory	Type	Description
description	No	String	Specifies supplementary information about the active/standby backend server group.
lb_algorithm	Yes	String	Specifies the load balancing algorithm used by the load balancer to route requests to backend servers in the associated backend server group. Value options: • **ROUND_ROBIN**: weighted round robin • **LEAST_CONNECTIONS**: weighted least connections • **SOURCE_IP**: source IP hash • **QUIC_CID**: connection ID
loadbalancer_id	No	String	Specifies the ID of the load balancer associated with the backend server group. Note: Specify at least one of **listener_id**, **loadbalancer_id**, or **type**.

Parameter	Mandatory	Type	Description
listener_id	No	String	Specifies the ID of the listener associated with the backend server group. Note: Specify at least one of **listener_id**, **loadbalancer_id**, or **type**.
name	No	String	Specifies the backend server group name.
project_id	No	String	Specifies the project ID of the backend server group.
protocol	Yes	String	Specifies the protocol used by the backend server group to receive requests. The value can be **TCP**, **UDP**, **QUIC**, or **TLS**. Note: • If the listener's protocol is **UDP**, the protocol of the backend server group must be **UDP** or **QUIC**. • If the listener's protocol is **TCP**, the protocol of the backend server group must be **TCP**. • If the listener's protocol is **QUIC**, the protocol of the backend server group can be **HTTP**, **HTTPS**, or **GRPC**. • If the listener's protocol is **TLS**, the protocol of the backend server group can be **TLS** or **TCP**. If protocol of the backend server group is TCP, the **ip_version** must be set to **v4**.
session_persistence	No	**CreatePoolSessionPersistenceOption** object	Specifies the sticky session.

Parameter	Mandatory	Type	Description
vpc_id	No	String	Specifies the ID of the VPC where the backend server group works. Note: • If **vpc_id** is not specified: – The backend server active/standby group must be associated with the VPC. – Only backend servers in the VPC or IP as backend servers can be added. – **type** must be set to **instance**. • If **vpc_id** is not specified: – **vpc_id** is determined by the VPC where the backend server works.
type	Yes	String	Specifies the type of the backend server group. Value options: • **instance**: Any type of backend servers can be added. **vpc_id** is mandatory. • **ip**: Only IP as backend servers can be added. **vpc_id** cannot be specified.
ip_version	No	String	Specifies the IP address version supported by the backend server group. • Shared load balancers: The value is fixed at **v4**. • Dedicated load balancers: The value can be **dualstack**, **v6**, or **v4**. If the protocol of the backend server group is TCP, UDP, or QUIC, the value is **dualstack**. If the protocol of the backend server group is HTTP, the value is **v4**.

Parameter	Mandatory	Type	Description
members	Yes	Array of **CreateMasterSlaveMemberOption** objects	Specifies the backend servers in the active/standby server group. Only two backend servers can be added, one serving as the active server and the other as the standby server.
healthmonitor	Yes	**CreateMasterSlaveHealthMonitorOption** object	Specifies the health check for active/standby backend server group. Health check is enabled by default and cannot be disabled.
any_port_enable	No	Boolean	Specifies whether to enable **any_port_enable** for a backend server group. If this option is enabled, the listener routes the requests to the backend server over the same port as the frontend port. If this option is disabled, the listener routes the requests over the port specified by **protocol_port**. Value options: • **false**: Disable this option. • **true**: Enable this option. Note: This option is available only for TCP, UDP, or QUIC backend server groups.
connection_drain	No	**ConnectionDrain** object	Specifies the configurations of deregistration delay. This parameter is only available for TCP, UDP, and QUIC backend server groups and TCP and UDP listeners. This parameter takes effect when: • A backend server is removed from a backend server group. • A backend server is detected unhealthy or health checks fail. • The weight of a backend server is 0.

Parameter	Mandatory	Type	Description
quic_cid_hash_strategy	No	QuicCidHashStrategy object	Specifies multi-path distribution configuration based on destination connection IDs.

Table 5-642 CreatePoolSessionPersistenceOption

Parameter	Mandatory	Type	Description
cookie_name	No	String	Specifies the cookie name. Note: • This parameter will take effect only when **type** is set to **APP_COOKIE**. Otherwise, an error will be returned. Value ranges: • For shared load balancers, the name can contain a maximum of 64 characters, including letters, digits, underscores (_), and hyphens (-). • For dedicated load balancers, the name can contain a maximum of 255 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).

Parameter	Mandatory	Type	Description
type	Yes	String	Specifies the sticky session type. The value can be **SOURCE_IP**, **HTTP_COOKIE**, or **APP_COOKIE**. Note: • If the protocol of the backend server group is **TCP** or **UDP**, only **SOURCE_IP** takes effect. • If the protocol of the backend server group is **HTTP** or **HTTPS**, the value can be **HTTP_COOKIE** or **APP_COOKIE**. • If the backend server group protocol is **QUIC**, sticky session must be enabled with **type** set to **SOURCE_IP**.
persistence_timeout	No	Integer	Specifies the stickiness duration, in minutes. This parameter will not take effect when **type** is set to **APP_COOKIE**. Value ranges: • If the protocol of the backend server group is TCP or UDP, the value ranges from **1** to **60**, and the default value is **1**. • If the protocol of the backend server group is HTTP or HTTPS, the value ranges from **1** to **1440**, and the default value is **1440**.

Table 5-643 CreateMasterSlaveMemberOption

Parameter	Mandatory	Type	Description
address	Yes	String	Specifies the private IP address bound to the backend server. Note: • If **subnet_cidr_id** is left blank, **IP as a Backend** is enabled. In this case, the IP address must be an IPv4 address. • If **subnet_cidr_id** is not left blank, the IP address can be IPv4 or IPv6. It must be in the subnet specified by **subnet_cidr_id**.
admin_state_up	No	Boolean	Specifies the administrative status of the backend server. The value can only be **true**. Although this parameter can be used in the APIs for creating and updating backend servers, its actual value depends on whether cloud servers exist. If cloud servers exist, the value is **true**. Otherwise, the value is **false**.
name	No	String	Specifies the backend server name.
protocol_port	No	Integer	Specifies the port used by the backend server to receive requests. **NOTE** This parameter can be left blank because it does not take effect if **any_port_enable** is set to **true** for a backend server group.

Parameter	Mandatory	Type	Description
subnet_cidr_id	No	String	Specifies the ID of the IPv4 or IPv6 subnet where the backend server resides. Note: • The IPv4 or IPv6 subnet must be in the same VPC as the subnet of the load balancer. • If this parameter is not passed, **IP as a Backend** has been enabled for the load balancer. In this case, IP as backend servers must use private IPv4 addresses, and the protocol of the backend server group must be TCP, UDP, TLS, HTTP, HTTPS, QUIC, or GRPC.
role	Yes	String	Specifies the type of the backend server. Value options: • **master**: active backend server • **slave**: standby backend server

Table 5-644 CreateMasterSlaveHealthMonitorOption

Parameter	Mandatory	Type	Description
delay	Yes	Integer	Specifies the interval between health checks, in seconds. The value ranges from **1** to **50**.

Parameter	Mandatory	Type	Description
domain_name	No	String	Specifies the domain name that HTTP requests are sent to during the health check. The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter. The value is left blank by default, indicating that the virtual IP address of the load balancer is used as the destination address of HTTP requests. This parameter is available only when **type** is set to **HTTP** or **HTTPS**.
expected_codes	No	String	Specifies the expected HTTP status code. This parameter will take effect only when **type** is set to **HTTP**, **HTTPS**, or **GRPC**. The value options are as follows: ● A specific value, for example, 200 ● A list of values that are separated with commas (,), for example, 200, 202 ● A value range, for example, 200-204 The default value is **200**.
http_method	No	String	Specifies the HTTP method. The value can be **GET**, **HEAD**, or **POST**. The default value is **GET**. This parameter is available when **type** is set to **HTTP** or **HTTPS**.
max_retries	Yes	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **OFFLINE** to **ONLINE**. The value ranges from **1** to **10**.

Parameter	Mandatory	Type	Description
max_retries_down	No	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **ONLINE** to **OFFLINE**. The value ranges from **1** to **10**, and the default value is **3**.
monitor_port	No	Integer	Specifies the port used for the health check. If this parameter is left blank, the port of the backend server will be used by default. The port number ranges from 1 to 65535.
name	No	String	Specifies the health check name.
timeout	Yes	Integer	Specifies the maximum time required for waiting for a response from the health check, in seconds. It is recommended that you set the value less than that of parameter **delay**.

Parameter	Mandatory	Type	Description
type	Yes	String	Specifies the health check protocol. The value can be **TCP**, **UDP_CONNECT**, **HTTP**, or **HTTPS**. Note: • If the protocol of the backend server is QUIC, the value can only be **UDP_CONNECT**. • If the protocol of the backend server is UDP, the value can only be **UDP_CONNECT**. • If the protocol of the backend server is TCP, the value can only be **TCP**, **HTTP**, or **HTTPS**. • If the protocol of the backend server is HTTP, the value can only be **TCP**, **HTTP**, or **HTTPS**. • If the protocol of the backend server is HTTPS, the value can only be **TCP**, **HTTP**, or **HTTPS**.
url_path	No	String	Specifies the HTTP request path for the health check. The value must start with a slash (/), and the default value is **/**. The value can contain letters, digits, hyphens (-), slashes (/), periods (.), percentage signs (%), question marks (?), pound signs (#), ampersand signs (&), and the extended character set: _;~!()*[]@$^:',+. Note: This parameter is available only when **type** is set to **HTTP** or **HTTPS**.

Table 5-645 ConnectionDrain

Parameter	Mandatory	Type	Description
enable	No	Boolean	Specifies whether to enable **connection_drain**. Value options: • **true**: Enable this option. • **false**: Disable this option. Default value: **true**
timeout	No	Integer	Specifies the deregistration delay timeout, in seconds. The value ranges from **10** to **4000**.

Table 5-646 QuicCidHashStrategy

Parameter	Mandatory	Type	Description
len	Yes	Integer	Specifies the length of the hash factor in the connection ID, in byte. This parameter is valid only when the load balancing algorithm is **QUIC_CID**. Value range: 1 to 20 Default value: 3
offset	Yes	Integer	Specifies the start position in the connection ID as the hash factor, in byte. This parameter is valid only when the load balancing algorithm is **QUIC_CID**. Value range: 0 to 19 Default value: 1

Response Parameters

Status code: 201

Table 5-647 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.

Parameter	Type	Description
pool	**MasterSlavePool** object	Specifies the active/standby backend server group.

Table 5-648 MasterSlavePool

Parameter	Type	Description
description	String	Specifies supplementary information about the active/standby backend server group.
id	String	Specifies the ID of the active/standby backend server group.
lb_algorithm	String	Specifies the load balancing algorithm used by the load balancer to route requests to backend servers in the associated backend server group. Value options: • **ROUND_ROBIN**: weighted round robin • **LEAST_CONNECTIONS**: weighted least connections • **SOURCE_IP**: source IP hash • **QUIC_CID**: connection ID Note: • If the value is **SOURCE_IP**, the **weight** parameter will not take effect for backend servers. • **QUIC_CID** is supported only when the protocol of the backend server group is QUIC.
listeners	Array of **ListenerRef** objects	Specifies the IDs of the listeners with which the backend server group is associated.
loadbalancers	Array of **LoadBalancerRef** objects	Specifies the IDs of the load balancers with which the backend server group is associated.
members	Array of **MasterSlaveMember** objects	Specifies the backend servers in the active/standby backend server group.
name	String	Specifies the backend server group name.

Parameter	Type	Description
project_id	String	Specifies the project ID.
protocol	String	Specifies the protocol used by the backend server group to receive requests. The value can be **TCP**, **UDP**, **QUIC**, or **TLS**. Note: • If the listener's protocol is **UDP**, the protocol of the backend server group must be **UDP** or **QUIC**. • If the listener's protocol is **TCP**, the protocol of the backend server group must be **TCP**. • If the listener's is **QUIC**, the protocol of the backend server group can be **HTTP**, **HTTPS**, or **GRPC**. • If the listener's protocol is **TLS**, the protocol of the backend server group can be **TLS** or **TCP**. If protocol of the backend server group is TCP, the **ip_version** must be set to **v4**.
session_persistence	**SessionPersistence** object	Specifies the sticky session.
ip_version	String	Specifies the IP address version supported by the backend server group. • Shared load balancers: The value is fixed at **v4**. • Dedicated load balancers: The value can be **dualstack** or **v4**. If the protocol of the backend server group is TCP, UDP, or QUIC, the value is **dualstack**. If the protocol of the backend server group is HTTP or HTTPS, the value is **v4**.

Parameter	Type	Description
created_at	String	Specifies the time when the backend server group was created. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
updated_at	String	Specifies the time when the backend server group was updated. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
vpc_id	String	Specifies the ID of the VPC where the active/standby backend server group works.
type	String	Specifies the type of the active/standby backend server group. Value options: • **instance**: Any type of backend servers can be added. **vpc_id** is mandatory. • **ip**: Only IP as backend servers can be added. **vpc_id** cannot be specified. • **""**: Any type of backend servers can be added.
enterprise_project_id	String	Specifies the enterprise project ID of the backend server group. All created projects belong to the default enterprise project.
healthmonitor	**MasterSlaveHealthMonitor** object	Specifies the health check configured for the active/standby backend server group.

Parameter	Type	Description
any_port_enable	Boolean	Specifies whether to enable **any_port_enable** for a backend server group. If this option is enabled, the listener routes the requests to the backend server over the same port as the frontend port. If this option is disabled, the listener routes the requests over the port specified by **protocol_port**. Value options: • **false**: Disable this option. • **true**: Enable this option. Note: This option is available only for TCP, UDP, or QUIC backend server groups.
connection_drain	**ConnectionDrain** object	Specifies the configurations of deregistration delay. This parameter is only available for TCP, UDP, and QUIC backend server groups and TCP and UDP listeners. This parameter takes effect when: • A backend server is removed from a backend server group. • A backend server is detected unhealthy or health checks fail. • The weight of a backend server is 0.
quic_cid_hash_strategy	**QuicCidHashStrategy** object	Specifies multi-path distribution configuration based on destination connection IDs.

Table 5-649 ListenerRef

Parameter	Type	Description
id	String	Specifies the listener ID.

Table 5-650 LoadBalancerRef

Parameter	Type	Description
id	String	Specifies the load balancer ID.

Table 5-651 MasterSlaveMember

Parameter	Type	Description
id	String	Specifies the backend server ID.
name	String	Specifies the backend server name.
admin_state_up	Boolean	Specifies the administrative status of the backend server. The value can be **true** or **false**. Although this parameter can be used in the APIs for creating and updating backend servers, its actual value depends on whether ECSs exist. If ECSs exist, the value is **true**. Otherwise, the value is **false**.
subnet_cidr_id	String	Specifies the ID of the IPv4 or IPv6 subnet where the backend server resides. This parameter can be left blank, indicating that **IP as a Backend** has been enabled for the load balancer. In this case, IP addresses of these servers must be IPv4 addresses, and the protocol of the backend server group must be UDP, TCP, TLS, HTTP, HTTPS, QUIC, or GRPC. The IPv4 or IPv6 subnet must be in the same VPC as the subnet of the load balancer.
protocol_port	Integer	Specifies the port used by the backend server to receive requests. **NOTE** This parameter can be left blank because it does not take effect if **any_port_enable** is set to **true** for a backend server group.
address	String	Specifies the private IP address bound to the backend server. Note: • If **subnet_cidr_id** is left blank, **IP as a Backend** is enabled. In this case, the IP address must be an IPv4 address. • If **subnet_cidr_id** is not left blank, the IP address can be IPv4 or IPv6. It must be in the subnet specified by **subnet_cidr_id**.

Parameter	Type	Description
ip_version	String	Specifies the IP version supported by the backend server. The value can be **v4** (IPv4) or **v6** (IPv6), depending on the value of **address** returned by the system.
device_owner	String	Specifies whether the backend server is associated with an ECS. • If this parameter is left blank, the backend server is not associated with an ECS. • If the value is **compute:{az_name}**, the backend server is associated with an ECS. **{az_name}** indicates the AZ where the ECS resides. This parameter is unsupported. Please do not use it.
device_id	String	Specifies the ID of the ECS with which the backend server is associated. If this parameter is left blank, the backend server is not associated with an ECS. This parameter is unsupported. Please do not use it.
operating_status	String	Specifies the health status of the backend server if **listener_id** under **status** is not specified. Value options: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group to which the backend server belongs. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist.
reason	**MemberHealthCheckFailedReason** object	Specifies why health check fails.

Parameter	Type	Description
member_type	String	Specifies the type of the backend server. Value options: • **ip**: IP as backend servers • **instance**: ECSs used as backend servers
instance_id	String	Specifies the ID of the instance associated with the backend server. If this parameter is left blank, the backend server is not a real device. It may be an IP address.
role	String	Specifies the type of the backend server.
status	Array of **ListenerMemberInfo** objects	Specifies the health status of the backend server if **listener_id** under **status** is specified. If **listener_id** under **status** is not specified, **operating_status** of **member** takes precedence.

Table 5-652 MemberHealthCheckFailedReason

Parameter	Type	Description
reason_code	String	Specifies the code of the health check failures. Value options: • **CONNECT_TIMEOUT**: The connection with the backend server times out during a health check. • **CONNECT_REFUSED**: The load balancer rejects connections with the backend server during a health check. • **CONNECT_FAILED**: The load balancer fails to establish connections with the backend server during a health check. • **CONNECT_INTERRUPT**: The load balancer is disconnected from the backend server during a health check. • **SSL_HANDSHAKE_ERROR**: The SSL handshakes with the backend server fail during a health check. • **RECV_RESPONSE_FAILED**: The load balancer fails to receive responses from the backend server during a health check. • **RECV_RESPONSE_TIMEOUT**: The load balancer does not receive responses from the backend server within the timeout duration during a health check. • **SEND_REQUEST_FAILED**: The load balancer fails to send a health check request to the backend server during a health check. • **SEND_REQUEST_TIMEOUT**: The load balancer fails to send a health check request to the backend server within the timeout duration. • **RESPONSE_FORMAT_ERROR**: The load balancer receives invalid responses from the backend server during a health check. • **RESPONSE_MISMATCH**: The response code received from the

Parameter	Type	Description
		backend server is different from the preset code.
expected_response	String	Specifies the expected HTTP status code. This parameter will take effect only when **type** is set to **HTTP**, **HTTPS**, or **GRPC**. The status code cannot be **null** if **reason_code** is **RESPONSE_MISMATCH**. Value ranges: ● A specific status code. If **type** is set to **GRPC**, the status code ranges from 0 to 99. If **type** is set to other values, the status code ranges from 200 to 599. For example, the status code can be **0** or **200**. ● A list of status codes that are separated with commas (,), for example, **200,202** or **0,1**. A maximum of five status codes are supported. ● A status code range. Different ranges are separated with commas (,), for example, **200-204,300-399** or **0-5,10-12,20-30**. A maximum of five ranges are supported.
healthcheck_response	String	Specifies the returned HTTP status code in the response. This parameter will take effect only when **type** is set to **HTTP**, **HTTPS**, or **GRPC**. The status code cannot be **null** if **reason_code** is **RESPONSE_MISMATCH**. Value range: A specific status code. If **type** is set to **GRPC**, the status code ranges from 0 to 99. If **type** is set to other values, the status code ranges from 200 to 599. For example, the status code can be **0** or **200**.

Table 5-653 ListenerMemberInfo

Parameter	Type	Description
listener_id	String	Specifies the ID of the listener associated with the backend server.
operating_status	String	Specifies the health status of the backend server. Value options: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group to which the backend server belongs. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist.

Table 5-654 SessionPersistence

Parameter	Type	Description
cookie_name	String	Specifies the cookie name. Note: • This parameter will take effect only when **type** is set to **APP_COOKIE**. Otherwise, an error will be returned. Value ranges: • For shared load balancers, the name can contain a maximum of 64 characters, including letters, digits, underscores (_), and hyphens (-). • For dedicated load balancers, the name can contain a maximum of 255 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).

Parameter	Type	Description
type	String	Specifies the sticky session type. The value can be **SOURCE_IP**, **HTTP_COOKIE**, or **APP_COOKIE**. Note: • If the protocol of the backend server group is **TCP** or **UDP**, only **SOURCE_IP** takes effect. • If the protocol of the backend server group is **HTTP** or **HTTPS**, the value can be **HTTP_COOKIE** or **APP_COOKIE**. • If the backend server group protocol is **QUIC**, sticky session must be enabled with **type** set to **SOURCE_IP**.
persistence_timeout	Integer	Specifies the stickiness duration, in minutes. This parameter will not take effect when **type** is set to **APP_COOKIE**. • If the protocol of the backend server group is TCP, UDP, or QUIC, the value ranges from **1** to **60**, and the default value is **1**. • If the protocol of the backend server group is HTTP or HTTPS, the value ranges from **1** to **1440**, and the default value is **1440**.

Table 5-655 MasterSlaveHealthMonitor

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the health check. • **true** (default) indicates that the health check is enabled. • **false** indicates that the health check is disabled.
delay	Integer	Specifies the interval between health checks, in seconds. The value ranges from **1** to **50**.

Parameter	Type	Description
domain_name	String	Specifies the domain name that HTTP requests are sent to during the health check. The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter. The value is left blank by default, indicating that the virtual IP address of the load balancer is used as the destination address of HTTP requests. This parameter is available only when **type** is set to **HTTP** or **HTTPS**.
expected_codes	String	Specifies the expected HTTP status code. This parameter will take effect only when **type** is set to **HTTP**, **HTTPS** or **GRPC**. The value options are as follows: ● A specific value, for example, 200 ● A list of values that are separated with commas (,), for example, 200, 202 ● A value range, for example, 200-204 The default value is **200**.
http_method	String	Specifies the HTTP method. The value can be **GET**, **HEAD**, or **POST**. The default value is **GET**. This parameter is available when **type** is set to **HTTP** or **HTTPS**.
id	String	Specifies the health check ID.
max_retries	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **OFFLINE** to **ONLINE**. The value ranges from **1** to **10**.
max_retries_down	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **ONLINE** to **OFFLINE**. The value ranges from **1** to **10**, and the default value is **3**.

Parameter	Type	Description
monitor_port	Integer	Specifies the port used for the health check. If this parameter is left blank, the port of the backend server will be used by default. The port number ranges from 1 to 65535.
name	String	Specifies the health check name.
timeout	Integer	Specifies the maximum time required for waiting for a response from the health check, in seconds. It is recommended that you set the value less than that of parameter **delay**.
type	String	Specifies the health check protocol. The value can be **TCP**, **UDP_CONNECT**, **HTTP**, or **HTTPS**. Note: ● If the protocol of the backend server is QUIC, the value can only be **UDP_CONNECT**. ● If the protocol of the backend server is UDP, the value can only be **UDP_CONNECT**. ● If the protocol of the backend server is TCP, the value can only be **TCP**, **HTTP**, or **HTTPS**. ● If the protocol of the backend server is HTTP, the value can only be **TCP**, **HTTP**, or **HTTPS**. ● If the protocol of the backend server is HTTPS, the value can only be **TCP**, **HTTP**, or **HTTPS**.
url_path	String	Specifies the HTTP request path for the health check. The value must start with a slash (/), and the default value is **/**. The value can contain letters, digits, hyphens (-), slashes (/), periods (.), percentage signs (%), question marks (?), pound signs (#), ampersand signs (&), and the extended character set: _;~!()*[]@$^:',+. Note: This parameter is available only when **type** is set to **HTTP** or **HTTPS**.

Table 5-656 ConnectionDrain

Parameter	Type	Description
enable	Boolean	Specifies whether to enable **connection_drain**. Value options: • **true**: Enable this option. • **false**: Disable this option. Default value: **true**
timeout	Integer	Specifies the deregistration delay timeout, in seconds. The value ranges from **10** to **4000**.

Table 5-657 QuicCidHashStrategy

Parameter	Type	Description
len	Integer	Specifies the length of the hash factor in the connection ID, in byte. This parameter is valid only when the load balancing algorithm is **QUIC_CID**. Value range: 1 to 20 Default value: 3
offset	Integer	Specifies the start position in the connection ID as the hash factor, in byte. This parameter is valid only when the load balancing algorithm is **QUIC_CID**. Value range: 0 to 19 Default value: 1

Example Requests

```
POST https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/master-slave-pools

{
  "pool" : {
    "name" : "My pool",
    "lb_algorithm" : "LEAST_CONNECTIONS",
    "listener_id" : "0b11747a-b139-492f-9692-2df0b1c87193",
    "protocol" : "TCP",
    "type" : "ip",
    "members" : [ {
      "protocol_port" : 89,
      "name" : "My member",
      "address" : "120.10.10.16",
      "role" : "master"
    }, {
      "protocol_port" : 89,
      "address" : "110.4.10.16",
```



```
    "role" : "slave"
   } ],
   "healthmonitor" : {
    "name" : "My Healthmonitor",
    "max_retries" : 3,
    "type" : "HTTP",
    "timeout" : 30,
    "delay" : 1
   }
  }
}
```

Example Responses

Status code: 201

Normal response to POST requests.

```
{
  "pool" : {
    "lb_algorithm" : "LEAST_CONNECTIONS",
    "type" : "ip",
    "vpc_id" : "3sae7086-a416-4666-9064-5b340e6840125",
    "protocol" : "TCP",
    "description" : "",
    "loadbalancers" : [ {
      "id" : "098b2f68-af1c-41a9-8efd-69958722af62"
    } ],
    "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
    "session_persistence" : null,
    "healthmonitor" : {
      "monitor_port" : null,
      "id" : "36ce7086-a496-4666-9064-5ba0e6840c75",
      "domain_name" : "",
      "name" : "My Healthmonitor",
      "max_retries" : 3,
      "max_retries_down" : 3,
      "admin_state_up" : true,
      "type" : "HTTP",
      "timeout" : 30,
      "delay" : 1,
      "http_method" : "get",
      "url_path" : "/",
      "expected_codes" : "200"
    },
    "listeners" : [ {
      "id" : "0b11747a-b139-492f-9692-2df0b1c87193"
    } ],
    "members" : [ {
      "admin_state_up" : true,
      "address" : "172.16.0.210",
      "protocol_port" : 80,
      "id" : "2e7b36d2-66c8-4825-bcd2-211d99978680",
      "operating_status" : "OFFLINE",
      "status" : [ {
        "listener_id" : "0b11747a-b139-492f-9692-2df0b1c87193",
        "operating_status" : "OFFLINE"
      } ],
      "instance_id" : "",
      "device_id" : "",
      "device_owner" : "",
      "member_type" : "ip",
      "role" : "master",
      "ip_version" : "v4",
      "name" : "cx-test-master",
      "subnet_cidr_id" : ""
    }, {
      "admin_state_up" : true,
      "address" : "172.16.0.211",
```



```
    "protocol_port" : 81,
    "id" : "2e7b36d2-66c8-4823-bsd2-21sa199978681",
    "operating_status" : "OFFLINE",
    "instance_id" : "",
    "device_id" : "",
    "device_owner" : "",
    "member_type" : "ip",
    "role" : "slave",
    "ip_version" : "v4",
    "name" : "cx-test-slave",
    "subnet_cidr_id" : "",
    "status" : [ {
      "listener_id" : "0b11747a-b139-492f-9692-2df0b1c87193",
      "operating_status" : "OFFLINE"
    } ]
  } ],
  "id" : "36ce7086-a496-4666-9064-5ba0e6840c75",
  "name" : "My pool",
  "ip_version" : "dualstack",
  "created_at" : "2021-03-26T01:33:12Z",
  "updated_at" : "2021-03-26T01:33:12Z"
 },
 "request_id" : "2d974978-0733-404d-a21a-b29204f4803a"
}
```


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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;

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

public class CreateMasterSlavePoolSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateMasterSlavePoolRequest request = new CreateMasterSlavePoolRequest();
        CreateMasterSlavePoolRequestBody body = new CreateMasterSlavePoolRequestBody();
```

```
        CreateMasterSlaveHealthMonitorOption healthmonitorPool = new
CreateMasterSlaveHealthMonitorOption();
        healthmonitorPool.withDelay(1)
            .withMaxRetries(3)
            .withName("My Healthmonitor")
            .withTimeout(30)
            .withType("HTTP");
        List<CreateMasterSlaveMemberOption> listPoolMembers = new ArrayList<>();
        listPoolMembers.add(
            new CreateMasterSlaveMemberOption()
                .withAddress("120.10.10.16")
                .withName("My member")
                .withProtocolPort(89)
                .withRole(CreateMasterSlaveMemberOption.RoleEnum.fromValue("master"))
        );
        listPoolMembers.add(
            new CreateMasterSlaveMemberOption()
                .withAddress("110.4.10.16")
                .withProtocolPort(89)
                .withRole(CreateMasterSlaveMemberOption.RoleEnum.fromValue("slave"))
        );
        CreateMasterSlavePoolOption poolbody = new CreateMasterSlavePoolOption();
        poolbody.withLbAlgorithm("LEAST_CONNECTIONS")
            .withListenerId("0b11747a-b139-492f-9692-2df0b1c87193")
            .withName("My pool")
            .withProtocol("TCP")
            .withType("ip")
            .withMembers(listPoolMembers)
            .withHealthmonitor(healthmonitorPool);
        body.withPool(poolbody);
        request.withBody(body);
        try {
            CreateMasterSlavePoolResponse response = client.createMasterSlavePool(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateMasterSlavePoolRequest()
        healthmonitorPool = CreateMasterSlaveHealthMonitorOption(
            delay=1,
            max_retries=3,
            name="My Healthmonitor",
            timeout=30,
            type="HTTP"
        )
        listMembersPool = [
            CreateMasterSlaveMemberOption(
                address="120.10.10.16",
                name="My member",
                protocol_port=89,
                role="master"
            ),
            CreateMasterSlaveMemberOption(
                address="110.4.10.16",
                protocol_port=89,
                role="slave"
            )
        ]
        poolbody = CreateMasterSlavePoolOption(
            lb_algorithm="LEAST_CONNECTIONS",
            listener_id="0b11747a-b139-492f-9692-2df0b1c87193",
            name="My pool",
            protocol="TCP",
            type="ip",
            members=listMembersPool,
            healthmonitor=healthmonitorPool
        )
        request.body = CreateMasterSlavePoolRequestBody(
            pool=poolbody
        )
        response = client.create_master_slave_pool(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateMasterSlavePoolRequest{}
    nameHealthmonitor:= "My Healthmonitor"
    healthmonitorPool := &model.CreateMasterSlaveHealthMonitorOption{
        Delay: int32(1),
        MaxRetries: int32(3),
        Name: &nameHealthmonitor,
        Timeout: int32(30),
        Type: "HTTP",
    }
    nameMembers:= "My member"
    protocolPortMembers:= int32(89)
    protocolPortMembers1:= int32(89)
    var listMembersPool = []model.CreateMasterSlaveMemberOption{
        {
            Address: "120.10.10.16",
            Name: &nameMembers,
            ProtocolPort: &protocolPortMembers,
            Role: model.GetCreateMasterSlaveMemberOptionRoleEnum().MASTER,
        },
        {
            Address: "110.4.10.16",
            ProtocolPort: &protocolPortMembers1,
            Role: model.GetCreateMasterSlaveMemberOptionRoleEnum().SLAVE,
        },
    }
    listenerIdPool:= "0b11747a-b139-492f-9692-2df0b1c87193"
    namePool:= "My pool"
    poolbody := &model.CreateMasterSlavePoolOption{
        LbAlgorithm: "LEAST_CONNECTIONS",
        ListenerId: &listenerIdPool,
        Name: &namePool,
        Protocol: "TCP",
        Type: "ip",
        Members: listMembersPool,
        Healthmonitor: healthmonitorPool,
    }
    request.Body = &model.CreateMasterSlavePoolRequestBody{
        Pool: poolbody,
    }
    response, err := client.CreateMasterSlavePool(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 POST requests.

Error Codes

See **Error Codes**.

5.16.2 Querying Active/Standby Backend Server Groups

Function

This API is used to query all active/standby backend server groups.

Constraints

This API has the following constraints:

- Parameters **marker**, **limit**, and **page_reverse** are used for pagination query.
- Parameters **marker** and **page_reverse** take effect only when they are used together with parameter **limit**.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/master-slave-pools

Table 5-658 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Table 5-659 Query Parameters

Parameter	Mandatory	Type	Description
marker	No	String	Specifies the ID of the last record on the previous page. Note: • This parameter must be used together with **limit**. • If this parameter is not specified, the first page will be queried. • This parameter cannot be left blank or set to an invalid ID.
limit	No	Integer	Specifies the number of records on each page. Value range: 0–2000 Default value: 2000
page_reverse	No	Boolean	Specifies whether to use reverse query. Value options: • **true**: Query the previous page. • **false** (default): Query the next page. Note: • This parameter must be used together with **limit**. • If **page_reverse** is set to **true** and you want to query the previous page, set the value of **marker** to the value of **previous_marker**.
description	No	Array of strings	Specifies supplementary information about the active/standby backend server group. Multiple descriptions can be queried in the format of *description=xxx&description=xxx*.

Parameter	Mandatory	Type	Description
healthmonitor_id	No	Array of strings	Specifies the ID of the health check configured for the active/standby backend server group. Multiple IDs can be queried in the format of *healthmonitor_id=xxx&healthmonitor_id=xxx*.
id	No	Array of strings	Specifies the ID of the active/standby backend server group. Multiple IDs can be queried in the format of *id=xxx&id=xxx*.
name	No	Array of strings	Specifies the name of the active/standby backend server group. Multiple names can be queried in the format of *name=xxx&name=xxx*.
loadbalancer_id	No	Array of strings	Specifies the ID of the load balancer with which the active/standby backend server group is associated. Multiple IDs can be queried in the format of *loadbalancer_id=xxx&loadbalancer_id=xxx*.
protocol	No	Array of strings	Specifies the protocol used by the backend server group to receive requests from the load balancer. The value can be **TCP**, **UDP**, **TLS**, **HTTP**, **HTTPS**, **GRPC**, or **QUIC**. Multiple protocols can be queried in the format of *protocol=xxx&protocol=xxx*.

Parameter	Mandatory	Type	Description
lb_algorithm	No	Array of strings	Specifies the load balancing algorithm used by the load balancer to route requests to backend servers in the associated backend server group. Value options: • **ROUND_ROBIN**: weighted round robin • **LEAST_CONNECTIONS**: weighted least connections • **SOURCE_IP**: source IP hash • **QUIC_CID**: connection ID Multiple algorithms can be queried in the format of *lb_algorithm=xxx&lb_algorithm=xxx*.
enterprise_project_id	No	Array of strings	Specifies the ID of the enterprise project. • If **enterprise_project_id** is not specified, resources in all enterprise projects are queried by default. Fine-grained authorization is performed. The **elb:pools:list** permission must be assigned to the user group. • If **enterprise_project_id** is specified, the value can be a specific enterprise project ID or **all_granted_eps**. If the value is a specific enterprise project ID, only resources in the enterprise project are queried. If the value is **all_granted_eps**, resources in the enterprise projects with the **elb:pools:list** permission are queried. Multiple values can be queried in the format of *enterprise_project_id=xxx&enterprise_project_id=xxx*.

Parameter	Mandatory	Type	Description
ip_version	No	Array of strings	Specifies the IP address version supported by the active/standby backend server group. Multiple versions can be queried in the format of *ip_version=xxx&ip_version=xxx*.
member_address	No	Array of strings	Specifies the private IP address bound to the backend server. This parameter is used only as a query condition and is not included in the response. Multiple IP addresses can be queried in the format of *member_address=xxx&member_address=xxx*.
member_device_id	No	Array of strings	Specifies the ID of the cloud server that serves as a backend server. This parameter is used only as a query condition and is not included in the response. Multiple IDs can be queried in the format of *member_device_id=xxx&member_device_id=xxx*.
listener_id	No	Array of strings	Specifies the IDs of the associated listeners, including the listeners associated through forwarding policies. Multiple IDs can be queried in the format of *listener_id=xxx&listener_id=xxx*.
member_instance_id	No	Array of strings	Specifies the backend server ID. This parameter is used only as a query condition and is not included in the response. Multiple IDs can be queried in the format of *member_instance_id=xxx&member_instance_id=xxx*.
vpc_id	No	Array of strings	Specifies the ID of the VPC where the active/standby backend server group works.

Parameter	Mandatory	Type	Description
type	No	Array of strings	Specifies the type of the active/standby backend server group. Value options: • **instance**: Any type of backend servers can be added. **vpc_id** is mandatory. • **ip**: Only IP as backend servers can be added. **vpc_id** cannot be specified. • **""**: Any type of backend servers can be added.
connection_drain	No	Boolean	Specifies a **connection_drain** value for query, in the format of **connection_drain=true** or **connection_drain=false**.

Request Parameters

Table 5-660 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-661 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
page_info	**PageInfo** object	Specifies the pagination information.
pools	Array of **MasterSlavePool** objects	Specifies the active/standby backend server groups.

Table 5-662 PageInfo

Parameter	Type	Description
previous_marker	String	Specifies the ID of the first record in the pagination query result. When **page_reverse** is set to **true**, this parameter is used together to query resources on the previous page.
next_marker	String	Specifies the ID of the last record in the pagination query result.
current_count	Integer	Specifies the number of records.

Table 5-663 MasterSlavePool

Parameter	Type	Description
description	String	Specifies supplementary information about the active/standby backend server group.
id	String	Specifies the ID of the active/standby backend server group.
lb_algorithm	String	Specifies the load balancing algorithm used by the load balancer to route requests to backend servers in the associated backend server group. Value options: • **ROUND_ROBIN**: weighted round robin • **LEAST_CONNECTIONS**: weighted least connections • **SOURCE_IP**: source IP hash • **QUIC_CID**: connection ID Note: • If the value is **SOURCE_IP**, the **weight** parameter will not take effect for backend servers. • **QUIC_CID** is supported only when the protocol of the backend server group is QUIC.
listeners	Array of **ListenerRef** objects	Specifies the IDs of the listeners with which the backend server group is associated.

Parameter	Type	Description
loadbalancers	Array of **LoadBalancerRef** objects	Specifies the IDs of the load balancers with which the backend server group is associated.
members	Array of **MasterSlaveMember** objects	Specifies the backend servers in the active/standby backend server group.
name	String	Specifies the backend server group name.
project_id	String	Specifies the project ID.
protocol	String	Specifies the protocol used by the backend server group to receive requests. The value can be **TCP**, **UDP**, **QUIC**, or **TLS**. Note: • If the listener's protocol is **UDP**, the protocol of the backend server group must be **UDP** or **QUIC**. • If the listener's protocol is **TCP**, the protocol of the backend server group must be **TCP**. • If the listener's is **QUIC**, the protocol of the backend server group can be **HTTP**, **HTTPS**, or **GRPC**. • If the listener's protocol is **TLS**, the protocol of the backend server group can be **TLS** or **TCP**. If protocol of the backend server group is TCP, the **ip_version** must be set to **v4**.
session_persistence	**SessionPersistence** object	Specifies the sticky session.

Parameter	Type	Description
ip_version	String	Specifies the IP address version supported by the backend server group. • Shared load balancers: The value is fixed at **v4**. • Dedicated load balancers: The value can be **dualstack** or **v4**. If the protocol of the backend server group is TCP, UDP, or QUIC, the value is **dualstack**. If the protocol of the backend server group is HTTP or HTTPS, the value is **v4**.
created_at	String	Specifies the time when the backend server group was created. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
updated_at	String	Specifies the time when the backend server group was updated. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
vpc_id	String	Specifies the ID of the VPC where the active/standby backend server group works.

Parameter	Type	Description
type	String	Specifies the type of the active/standby backend server group. Value options: • **instance**: Any type of backend servers can be added. **vpc_id** is mandatory. • **ip**: Only IP as backend servers can be added. **vpc_id** cannot be specified. • **""**: Any type of backend servers can be added.
enterprise_project_id	String	Specifies the enterprise project ID of the backend server group. All created projects belong to the default enterprise project.
healthmonitor	**MasterSlaveHealthMonitor** object	Specifies the health check configured for the active/standby backend server group.
any_port_enable	Boolean	Specifies whether to enable **any_port_enable** for a backend server group. If this option is enabled, the listener routes the requests to the backend server over the same port as the frontend port. If this option is disabled, the listener routes the requests over the port specified by **protocol_port**. Value options: • **false**: Disable this option. • **true**: Enable this option. Note: This option is available only for TCP, UDP, or QUIC backend server groups.
connection_drain	**ConnectionDrain** object	Specifies the configurations of deregistration delay. This parameter is only available for TCP, UDP, and QUIC backend server groups and TCP and UDP listeners. This parameter takes effect when: • A backend server is removed from a backend server group. • A backend server is detected unhealthy or health checks fail. • The weight of a backend server is 0.

Parameter	Type	Description
quic_cid_hash_strategy	**QuicCidHashStrategy** object	Specifies multi-path distribution configuration based on destination connection IDs.

Table 5-664 ListenerRef

Parameter	Type	Description
id	String	Specifies the listener ID.

Table 5-665 LoadBalancerRef

Parameter	Type	Description
id	String	Specifies the load balancer ID.

Table 5-666 MasterSlaveMember

Parameter	Type	Description
id	String	Specifies the backend server ID.
name	String	Specifies the backend server name.
admin_state_up	Boolean	Specifies the administrative status of the backend server. The value can be **true** or **false**. Although this parameter can be used in the APIs for creating and updating backend servers, its actual value depends on whether ECSs exist. If ECSs exist, the value is **true**. Otherwise, the value is **false**.

Parameter	Type	Description
subnet_cidr_id	String	Specifies the ID of the IPv4 or IPv6 subnet where the backend server resides. This parameter can be left blank, indicating that **IP as a Backend** has been enabled for the load balancer. In this case, IP addresses of these servers must be IPv4 addresses, and the protocol of the backend server group must be UDP, TCP, TLS, HTTP, HTTPS, QUIC, or GRPC. The IPv4 or IPv6 subnet must be in the same VPC as the subnet of the load balancer.
protocol_port	Integer	Specifies the port used by the backend server to receive requests. **NOTE** This parameter can be left blank because it does not take effect if **any_port_enable** is set to **true** for a backend server group.
address	String	Specifies the private IP address bound to the backend server. Note: • If **subnet_cidr_id** is left blank, **IP as a Backend** is enabled. In this case, the IP address must be an IPv4 address. • If **subnet_cidr_id** is not left blank, the IP address can be IPv4 or IPv6. It must be in the subnet specified by **subnet_cidr_id**.
ip_version	String	Specifies the IP version supported by the backend server. The value can be **v4** (IPv4) or **v6** (IPv6), depending on the value of **address** returned by the system.

Parameter	Type	Description
device_owner	String	Specifies whether the backend server is associated with an ECS. • If this parameter is left blank, the backend server is not associated with an ECS. • If the value is **compute:{az_name}**, the backend server is associated with an ECS. **{az_name}** indicates the AZ where the ECS resides. This parameter is unsupported. Please do not use it.
device_id	String	Specifies the ID of the ECS with which the backend server is associated. If this parameter is left blank, the backend server is not associated with an ECS. This parameter is unsupported. Please do not use it.
operating_status	String	Specifies the health status of the backend server if **listener_id** under **status** is not specified. Value options: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group to which the backend server belongs. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist.
reason	**MemberHealthCheckFailedReason** object	Specifies why health check fails.
member_type	String	Specifies the type of the backend server. Value options: • **ip**: IP as backend servers • **instance**: ECSs used as backend servers

Parameter	Type	Description
instance_id	String	Specifies the ID of the instance associated with the backend server. If this parameter is left blank, the backend server is not a real device. It may be an IP address.
role	String	Specifies the type of the backend server.
status	Array of **ListenerMemberInfo** objects	Specifies the health status of the backend server if **listener_id** under **status** is specified. If **listener_id** under **status** is not specified, **operating_status** of **member** takes precedence.

Table 5-667 MemberHealthCheckFailedReason

Parameter	Type	Description
reason_code	String	Specifies the code of the health check failures. Value options: • **CONNECT_TIMEOUT**: The connection with the backend server times out during a health check. • **CONNECT_REFUSED**: The load balancer rejects connections with the backend server during a health check. • **CONNECT_FAILED**: The load balancer fails to establish connections with the backend server during a health check. • **CONNECT_INTERRUPT**: The load balancer is disconnected from the backend server during a health check. • **SSL_HANDSHAKE_ERROR**: The SSL handshakes with the backend server fail during a health check. • **RECV_RESPONSE_FAILED**: The load balancer fails to receive responses from the backend server during a health check. • **RECV_RESPONSE_TIMEOUT**: The load balancer does not receive responses from the backend server within the timeout duration during a health check. • **SEND_REQUEST_FAILED**: The load balancer fails to send a health check request to the backend server during a health check. • **SEND_REQUEST_TIMEOUT**: The load balancer fails to send a health check request to the backend server within the timeout duration. • **RESPONSE_FORMAT_ERROR**: The load balancer receives invalid responses from the backend server during a health check. • **RESPONSE_MISMATCH**: The response code received from the

Parameter	Type	Description
		backend server is different from the preset code.
expected_response	String	Specifies the expected HTTP status code. This parameter will take effect only when **type** is set to **HTTP**, **HTTPS**, or **GRPC**. The status code cannot be **null** if **reason_code** is **RESPONSE_MISMATCH**. Value ranges: ● A specific status code. If **type** is set to **GRPC**, the status code ranges from 0 to 99. If **type** is set to other values, the status code ranges from 200 to 599. For example, the status code can be **0** or **200**. ● A list of status codes that are separated with commas (,), for example, **200,202** or **0,1**. A maximum of five status codes are supported. ● A status code range. Different ranges are separated with commas (,), for example, **200-204,300-399** or **0-5,10-12,20-30**. A maximum of five ranges are supported.
healthcheck_response	String	Specifies the returned HTTP status code in the response. This parameter will take effect only when **type** is set to **HTTP**, **HTTPS**, or **GRPC**. The status code cannot be **null** if **reason_code** is **RESPONSE_MISMATCH**. Value range: A specific status code. If **type** is set to **GRPC**, the status code ranges from 0 to 99. If **type** is set to other values, the status code ranges from 200 to 599. For example, the status code can be **0** or **200**.

Table 5-668 ListenerMemberInfo

Parameter	Type	Description
listener_id	String	Specifies the ID of the listener associated with the backend server.
operating_status	String	Specifies the health status of the backend server. Value options: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group to which the backend server belongs. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist.

Table 5-669 SessionPersistence

Parameter	Type	Description
cookie_name	String	Specifies the cookie name. Note: • This parameter will take effect only when **type** is set to **APP_COOKIE**. Otherwise, an error will be returned. Value ranges: • For shared load balancers, the name can contain a maximum of 64 characters, including letters, digits, underscores (_), and hyphens (-). • For dedicated load balancers, the name can contain a maximum of 255 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).

Parameter	Type	Description
type	String	Specifies the sticky session type. The value can be **SOURCE_IP**, **HTTP_COOKIE**, or **APP_COOKIE**. Note: • If the protocol of the backend server group is **TCP** or **UDP**, only **SOURCE_IP** takes effect. • If the protocol of the backend server group is **HTTP** or **HTTPS**, the value can be **HTTP_COOKIE** or **APP_COOKIE**. • If the backend server group protocol is **QUIC**, sticky session must be enabled with **type** set to **SOURCE_IP**.
persistence_timeout	Integer	Specifies the stickiness duration, in minutes. This parameter will not take effect when **type** is set to **APP_COOKIE**. • If the protocol of the backend server group is TCP, UDP, or QUIC, the value ranges from **1** to **60**, and the default value is **1**. • If the protocol of the backend server group is HTTP or HTTPS, the value ranges from **1** to **1440**, and the default value is **1440**.

Table 5-670 MasterSlaveHealthMonitor

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the health check. • **true** (default) indicates that the health check is enabled. • **false** indicates that the health check is disabled.
delay	Integer	Specifies the interval between health checks, in seconds. The value ranges from **1** to **50**.

Parameter	Type	Description
domain_name	String	Specifies the domain name that HTTP requests are sent to during the health check. The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter. The value is left blank by default, indicating that the virtual IP address of the load balancer is used as the destination address of HTTP requests. This parameter is available only when **type** is set to **HTTP** or **HTTPS**.
expected_codes	String	Specifies the expected HTTP status code. This parameter will take effect only when **type** is set to **HTTP**, **HTTPS** or **GRPC**. The value options are as follows: ● A specific value, for example, 200 ● A list of values that are separated with commas (,), for example, 200, 202 ● A value range, for example, 200-204 The default value is **200**.
http_method	String	Specifies the HTTP method. The value can be **GET**, **HEAD**, or **POST**. The default value is **GET**. This parameter is available when **type** is set to **HTTP** or **HTTPS**.
id	String	Specifies the health check ID.
max_retries	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **OFFLINE** to **ONLINE**. The value ranges from **1** to **10**.
max_retries_down	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **ONLINE** to **OFFLINE**. The value ranges from **1** to **10**, and the default value is **3**.

Parameter	Type	Description
monitor_port	Integer	Specifies the port used for the health check. If this parameter is left blank, the port of the backend server will be used by default. The port number ranges from 1 to 65535.
name	String	Specifies the health check name.
timeout	Integer	Specifies the maximum time required for waiting for a response from the health check, in seconds. It is recommended that you set the value less than that of parameter **delay**.
type	String	Specifies the health check protocol. The value can be **TCP**, **UDP_CONNECT**, **HTTP**, or **HTTPS**. Note: ● If the protocol of the backend server is QUIC, the value can only be **UDP_CONNECT**. ● If the protocol of the backend server is UDP, the value can only be **UDP_CONNECT**. ● If the protocol of the backend server is TCP, the value can only be **TCP**, **HTTP**, or **HTTPS**. ● If the protocol of the backend server is HTTP, the value can only be **TCP**, **HTTP**, or **HTTPS**. ● If the protocol of the backend server is HTTPS, the value can only be **TCP**, **HTTP**, or **HTTPS**.
url_path	String	Specifies the HTTP request path for the health check. The value must start with a slash (/), and the default value is **/**. The value can contain letters, digits, hyphens (-), slashes (/), periods (.), percentage signs (%), question marks (?), pound signs (#), ampersand signs (&), and the extended character set: _;~!()*[]@$^:',+. Note: This parameter is available only when **type** is set to **HTTP** or **HTTPS**.

Table 5-671 ConnectionDrain

Parameter	Type	Description
enable	Boolean	Specifies whether to enable **connection_drain**. Value options: • **true**: Enable this option. • **false**: Disable this option. Default value: **true**
timeout	Integer	Specifies the deregistration delay timeout, in seconds. The value ranges from **10** to **4000**.

Table 5-672 QuicCidHashStrategy

Parameter	Type	Description
len	Integer	Specifies the length of the hash factor in the connection ID, in byte. This parameter is valid only when the load balancing algorithm is **QUIC_CID**. Value range: 1 to 20 Default value: 3
offset	Integer	Specifies the start position in the connection ID as the hash factor, in byte. This parameter is valid only when the load balancing algorithm is **QUIC_CID**. Value range: 0 to 19 Default value: 1

Example Requests

```
GET https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/master-slave-pools?limit=2
```

Example Responses

Status code: 200

Successful request.

```
{
  "pools" : [ {
    "lb_algorithm" : "ROUND_ROBIN",
    "protocol" : "HTTP",
    "description" : "",
    "loadbalancers" : [ {
      "id" : "309a0f61-0b62-45f2-97d1-742f3434338e"
    } ],
```



```
  "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
  "session_persistence" : {
    "cookie_name" : "my_cookie",
    "type" : "APP_COOKIE",
    "persistence_timeout" : 1
  },
  "healthmonitor" : {
    "monitor_port" : null,
    "id" : "36ce7086-a496-4666-9064-5ba0e6840c75",
    "domain_name" : "",
    "name" : "My Healthmonitor",
    "max_retries" : 3,
    "max_retries_down" : 3,
    "admin_state_up" : true,
    "type" : "HTTP",
    "timeout" : 30,
    "delay" : 1,
    "http_method" : "get",
    "url_path" : "/",
    "expected_codes" : "200"
  },
  "listeners" : [ ],
  "members" : [ {
    "admin_state_up" : true,
    "address" : "172.16.0.210",
    "protocol_port" : 80,
    "id" : "2e7b36d2-66c8-4825-bcd2-211d99978680",
    "operating_status" : "OFFLINE",
    "status" : [ ],
    "instance_id" : "",
    "device_id" : "",
    "device_owner" : "",
    "member_type" : "ip",
    "role" : "master",
    "ip_version" : "v4",
    "name" : "cx-test-master",
    "subnet_cidr_id" : ""
  }, {
    "admin_state_up" : true,
    "address" : "172.16.0.211",
    "protocol_port" : 81,
    "id" : "2e7b36d2-66c8-4823-bsd2-21sa199978681",
    "operating_status" : "OFFLINE",
    "status" : [ ],
    "instance_id" : "",
    "device_id" : "",
    "device_owner" : "",
    "member_type" : "ip",
    "role" : "slave",
    "ip_version" : "v4",
    "name" : "cx-test-slave",
    "subnet_cidr_id" : ""
  } ],
  "id" : "73bd4fe0-ffbb-4b56-aab4-4f26ddf7a103",
  "name" : "",
  "ip_version" : "v4",
  "type" : "ip",
  "vpc_id" : "",
  "created_at" : "2021-03-26T01:33:12Z",
  "updated_at" : "2021-03-26T01:33:12Z"
}, {
  "lb_algorithm" : "SOURCE_IP",
  "protocol" : "TCP",
  "description" : "",
  "loadbalancers" : [ {
    "id" : "d9763e59-64b7-4e93-aec7-0ff7881ef9bc"
  } ],
  "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
  "session_persistence" : {
```



```
    "cookie_name" : "",
    "type" : "SOURCE_IP",
    "persistence_timeout" : 1
  },
  "healthmonitor" : {
    "monitor_port" : null,
    "id" : "36ce7086-a496-4666-9064-5ba0e6840c75",
    "domain_name" : "",
    "name" : "My Healthmonitor",
    "max_retries" : 3,
    "max_retries_down" : 3,
    "admin_state_up" : true,
    "type" : "HTTP",
    "timeout" : 30,
    "delay" : 1,
    "http_method" : "get",
    "url_path" : "/",
    "expected_codes" : "200"
  },
  "listeners" : [ {
    "id" : "8d21db6f-b475-429e-a9cb-90439b0413b2"
  } ],
  "members" : [ {
    "admin_state_up" : true,
    "address" : "172.16.1.210",
    "protocol_port" : 83,
    "id" : "2e7b36d2-9997-4825-bcd2-211d9990439b",
    "operating_status" : "OFFLINE",
    "status" : [ ],
    "instance_id" : "",
    "device_id" : "",
    "device_owner" : "",
    "member_type" : "ip",
    "role" : "master",
    "ip_version" : "v4",
    "name" : "cx-test-master",
    "subnet_cidr_id" : ""
  }, {
    "admin_state_up" : true,
    "address" : "172.16.1.212",
    "protocol_port" : 82,
    "id" : "227b31d2-66c1-4823-bsd2-21sa199978213",
    "operating_status" : "OFFLINE",
    "status" : [ ],
    "instance_id" : "",
    "device_id" : "",
    "device_owner" : "",
    "member_type" : "ip",
    "role" : "slave",
    "ip_version" : "v4",
    "name" : "cx-test-slave",
    "subnet_cidr_id" : ""
  } ],
  "id" : "74db02d1-5711-4c77-b383-a450e2b93142",
  "name" : "pool_tcp_001",
  "ip_version" : "dualstack",
  "type" : "ip",
  "vpc_id" : "",
  "created_at" : "2021-03-26T01:33:12Z",
  "updated_at" : "2021-03-26T01:33:12Z"
 } ],
 "page_info" : {
  "next_marker" : "74db02d1-5711-4c77-b383-a450e2b93142",
  "previous_marker" : "73bd4fe0-ffbb-4b56-aab4-4f26ddf7a103",
  "current_count" : 2
 },
 "request_id" : "a1a7e852-1928-48f7-bbc9-ca8469898713"
}
```


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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ListMasterSlavePoolsSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ListMasterSlavePoolsRequest request = new ListMasterSlavePoolsRequest();
        try {
            ListMasterSlavePoolsResponse response = client.listMasterSlavePools(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListMasterSlavePoolsRequest()
        response = client.list_master_slave_pools(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListMasterSlavePoolsRequest{}
    response, err := client.ListMasterSlavePools(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	Successful request.

Error Codes

See **Error Codes**.

5.16.3 Viewing the Details of an Active/Standby Backend Server Group

Function

This API is used to view the details of an active/standby backend server group.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/master-slave-pools/{pool_id}

Table 5-673 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
pool_id	Yes	String	Specifies the ID of the active/standby backend server group.

Request Parameters

Table 5-674 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-675 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
pool	**MasterSlavePool** object	Specifies the active/standby backend server group.

Table 5-676 MasterSlavePool

Parameter	Type	Description
description	String	Specifies supplementary information about the active/standby backend server group.
id	String	Specifies the ID of the active/standby backend server group.
lb_algorithm	String	Specifies the load balancing algorithm used by the load balancer to route requests to backend servers in the associated backend server group. Value options: • **ROUND_ROBIN**: weighted round robin • **LEAST_CONNECTIONS**: weighted least connections • **SOURCE_IP**: source IP hash • **QUIC_CID**: connection ID Note: • If the value is **SOURCE_IP**, the **weight** parameter will not take effect for backend servers. • **QUIC_CID** is supported only when the protocol of the backend server group is QUIC.
listeners	Array of **ListenerRef** objects	Specifies the IDs of the listeners with which the backend server group is associated.

Parameter	Type	Description
loadbalancers	Array of **LoadBalancerRef** objects	Specifies the IDs of the load balancers with which the backend server group is associated.
members	Array of **MasterSlaveMember** objects	Specifies the backend servers in the active/standby backend server group.
name	String	Specifies the backend server group name.
project_id	String	Specifies the project ID.
protocol	String	Specifies the protocol used by the backend server group to receive requests. The value can be **TCP**, **UDP**, **QUIC**, or **TLS**. Note: • If the listener's protocol is **UDP**, the protocol of the backend server group must be **UDP** or **QUIC**. • If the listener's protocol is **TCP**, the protocol of the backend server group must be **TCP**. • If the listener's is **QUIC**, the protocol of the backend server group can be **HTTP**, **HTTPS**, or **GRPC**. • If the listener's protocol is **TLS**, the protocol of the backend server group can be **TLS** or **TCP**. If protocol of the backend server group is TCP, the **ip_version** must be set to **v4**.
session_persistence	**SessionPersistence** object	Specifies the sticky session.

Parameter	Type	Description
ip_version	String	Specifies the IP address version supported by the backend server group. • Shared load balancers: The value is fixed at **v4**. • Dedicated load balancers: The value can be **dualstack** or **v4**. If the protocol of the backend server group is TCP, UDP, or QUIC, the value is **dualstack**. If the protocol of the backend server group is HTTP or HTTPS, the value is **v4**.
created_at	String	Specifies the time when the backend server group was created. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
updated_at	String	Specifies the time when the backend server group was updated. The format is yyyy-MM-dd'T'HH:mm:ss'Z' (UTC time). This is a new field in this version, and it will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
vpc_id	String	Specifies the ID of the VPC where the active/standby backend server group works.

Parameter	Type	Description
type	String	Specifies the type of the active/standby backend server group. Value options: • **instance**: Any type of backend servers can be added. **vpc_id** is mandatory. • **ip**: Only IP as backend servers can be added. **vpc_id** cannot be specified. • **""**: Any type of backend servers can be added.
enterprise_project_id	String	Specifies the enterprise project ID of the backend server group. All created projects belong to the default enterprise project.
healthmonitor	**MasterSlaveHealthMonitor** object	Specifies the health check configured for the active/standby backend server group.
any_port_enable	Boolean	Specifies whether to enable **any_port_enable** for a backend server group. If this option is enabled, the listener routes the requests to the backend server over the same port as the frontend port. If this option is disabled, the listener routes the requests over the port specified by **protocol_port**. Value options: • **false**: Disable this option. • **true**: Enable this option. Note: This option is available only for TCP, UDP, or QUIC backend server groups.
connection_drain	**ConnectionDrain** object	Specifies the configurations of deregistration delay. This parameter is only available for TCP, UDP, and QUIC backend server groups and TCP and UDP listeners. This parameter takes effect when: • A backend server is removed from a backend server group. • A backend server is detected unhealthy or health checks fail. • The weight of a backend server is 0.

Parameter	Type	Description
quic_cid_hash_strategy	**QuicCidHashStrategy** object	Specifies multi-path distribution configuration based on destination connection IDs.

Table 5-677 ListenerRef

Parameter	Type	Description
id	String	Specifies the listener ID.

Table 5-678 LoadBalancerRef

Parameter	Type	Description
id	String	Specifies the load balancer ID.

Table 5-679 MasterSlaveMember

Parameter	Type	Description
id	String	Specifies the backend server ID.
name	String	Specifies the backend server name.
admin_state_up	Boolean	Specifies the administrative status of the backend server. The value can be **true** or **false**. Although this parameter can be used in the APIs for creating and updating backend servers, its actual value depends on whether ECSs exist. If ECSs exist, the value is **true**. Otherwise, the value is **false**.

Parameter	Type	Description
subnet_cidr_id	String	Specifies the ID of the IPv4 or IPv6 subnet where the backend server resides. This parameter can be left blank, indicating that **IP as a Backend** has been enabled for the load balancer. In this case, IP addresses of these servers must be IPv4 addresses, and the protocol of the backend server group must be UDP, TCP, TLS, HTTP, HTTPS, QUIC, or GRPC. The IPv4 or IPv6 subnet must be in the same VPC as the subnet of the load balancer.
protocol_port	Integer	Specifies the port used by the backend server to receive requests. **NOTE** This parameter can be left blank because it does not take effect if **any_port_enable** is set to **true** for a backend server group.
address	String	Specifies the private IP address bound to the backend server. Note: • If **subnet_cidr_id** is left blank, **IP as a Backend** is enabled. In this case, the IP address must be an IPv4 address. • If **subnet_cidr_id** is not left blank, the IP address can be IPv4 or IPv6. It must be in the subnet specified by **subnet_cidr_id**.
ip_version	String	Specifies the IP version supported by the backend server. The value can be **v4** (IPv4) or **v6** (IPv6), depending on the value of **address** returned by the system.

Parameter	Type	Description
device_owner	String	Specifies whether the backend server is associated with an ECS. • If this parameter is left blank, the backend server is not associated with an ECS. • If the value is **compute:{az_name}**, the backend server is associated with an ECS. **{az_name}** indicates the AZ where the ECS resides. This parameter is unsupported. Please do not use it.
device_id	String	Specifies the ID of the ECS with which the backend server is associated. If this parameter is left blank, the backend server is not associated with an ECS. This parameter is unsupported. Please do not use it.
operating_status	String	Specifies the health status of the backend server if **listener_id** under **status** is not specified. Value options: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group to which the backend server belongs. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist.
reason	**MemberHealthCheckFailedReason** object	Specifies why health check fails.
member_type	String	Specifies the type of the backend server. Value options: • **ip**: IP as backend servers • **instance**: ECSs used as backend servers

Parameter	Type	Description
instance_id	String	Specifies the ID of the instance associated with the backend server. If this parameter is left blank, the backend server is not a real device. It may be an IP address.
role	String	Specifies the type of the backend server.
status	Array of **ListenerMemberInfo** objects	Specifies the health status of the backend server if **listener_id** under **status** is specified. If **listener_id** under **status** is not specified, **operating_status** of **member** takes precedence.

Table 5-680 MemberHealthCheckFailedReason

Parameter	Type	Description
reason_code	String	Specifies the code of the health check failures. Value options: • **CONNECT_TIMEOUT**: The connection with the backend server times out during a health check. • **CONNECT_REFUSED**: The load balancer rejects connections with the backend server during a health check. • **CONNECT_FAILED**: The load balancer fails to establish connections with the backend server during a health check. • **CONNECT_INTERRUPT**: The load balancer is disconnected from the backend server during a health check. • **SSL_HANDSHAKE_ERROR**: The SSL handshakes with the backend server fail during a health check. • **RECV_RESPONSE_FAILED**: The load balancer fails to receive responses from the backend server during a health check. • **RECV_RESPONSE_TIMEOUT**: The load balancer does not receive responses from the backend server within the timeout duration during a health check. • **SEND_REQUEST_FAILED**: The load balancer fails to send a health check request to the backend server during a health check. • **SEND_REQUEST_TIMEOUT**: The load balancer fails to send a health check request to the backend server within the timeout duration. • **RESPONSE_FORMAT_ERROR**: The load balancer receives invalid responses from the backend server during a health check. • **RESPONSE_MISMATCH**: The response code received from the

Parameter	Type	Description
		backend server is different from the preset code.
expected_response	String	Specifies the expected HTTP status code. This parameter will take effect only when **type** is set to **HTTP**, **HTTPS**, or **GRPC**. The status code cannot be **null** if **reason_code** is **RESPONSE_MISMATCH**. Value ranges: ● A specific status code. If **type** is set to **GRPC**, the status code ranges from 0 to 99. If **type** is set to other values, the status code ranges from 200 to 599. For example, the status code can be **0** or **200**. ● A list of status codes that are separated with commas (,), for example, **200,202** or **0,1**. A maximum of five status codes are supported. ● A status code range. Different ranges are separated with commas (,), for example, **200-204,300-399** or **0-5,10-12,20-30**. A maximum of five ranges are supported.
healthcheck_response	String	Specifies the returned HTTP status code in the response. This parameter will take effect only when **type** is set to **HTTP**, **HTTPS**, or **GRPC**. The status code cannot be **null** if **reason_code** is **RESPONSE_MISMATCH**. Value range: A specific status code. If **type** is set to **GRPC**, the status code ranges from 0 to 99. If **type** is set to other values, the status code ranges from 200 to 599. For example, the status code can be **0** or **200**.

Table 5-681 ListenerMemberInfo

Parameter	Type	Description
listener_id	String	Specifies the ID of the listener associated with the backend server.
operating_status	String	Specifies the health status of the backend server. Value options: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group to which the backend server belongs. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist.

Table 5-682 SessionPersistence

Parameter	Type	Description
cookie_name	String	Specifies the cookie name. Note: • This parameter will take effect only when **type** is set to **APP_COOKIE**. Otherwise, an error will be returned. Value ranges: • For shared load balancers, the name can contain a maximum of 64 characters, including letters, digits, underscores (_), and hyphens (-). • For dedicated load balancers, the name can contain a maximum of 255 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).

Parameter	Type	Description
type	String	Specifies the sticky session type. The value can be **SOURCE_IP**, **HTTP_COOKIE**, or **APP_COOKIE**. Note: • If the protocol of the backend server group is **TCP** or **UDP**, only **SOURCE_IP** takes effect. • If the protocol of the backend server group is **HTTP** or **HTTPS**, the value can be **HTTP_COOKIE** or **APP_COOKIE**. • If the backend server group protocol is **QUIC**, sticky session must be enabled with **type** set to **SOURCE_IP**.
persistence_timeout	Integer	Specifies the stickiness duration, in minutes. This parameter will not take effect when **type** is set to **APP_COOKIE**. • If the protocol of the backend server group is TCP, UDP, or QUIC, the value ranges from **1** to **60**, and the default value is **1**. • If the protocol of the backend server group is HTTP or HTTPS, the value ranges from **1** to **1440**, and the default value is **1440**.

Table 5-683 MasterSlaveHealthMonitor

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the health check. • **true** (default) indicates that the health check is enabled. • **false** indicates that the health check is disabled.
delay	Integer	Specifies the interval between health checks, in seconds. The value ranges from **1** to **50**.

Parameter	Type	Description
domain_name	String	Specifies the domain name that HTTP requests are sent to during the health check. The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter. The value is left blank by default, indicating that the virtual IP address of the load balancer is used as the destination address of HTTP requests. This parameter is available only when **type** is set to **HTTP** or **HTTPS**.
expected_codes	String	Specifies the expected HTTP status code. This parameter will take effect only when **type** is set to **HTTP**, **HTTPS** or **GRPC**. The value options are as follows: ● A specific value, for example, 200 ● A list of values that are separated with commas (,), for example, 200, 202 ● A value range, for example, 200-204 The default value is **200**.
http_method	String	Specifies the HTTP method. The value can be **GET**, **HEAD**, or **POST**. The default value is **GET**. This parameter is available when **type** is set to **HTTP** or **HTTPS**.
id	String	Specifies the health check ID.
max_retries	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **OFFLINE** to **ONLINE**. The value ranges from **1** to **10**.
max_retries_down	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **ONLINE** to **OFFLINE**. The value ranges from **1** to **10**, and the default value is **3**.

Parameter	Type	Description
monitor_port	Integer	Specifies the port used for the health check. If this parameter is left blank, the port of the backend server will be used by default. The port number ranges from 1 to 65535.
name	String	Specifies the health check name.
timeout	Integer	Specifies the maximum time required for waiting for a response from the health check, in seconds. It is recommended that you set the value less than that of parameter **delay**.
type	String	Specifies the health check protocol. The value can be **TCP**, **UDP_CONNECT**, **HTTP**, or **HTTPS**. Note: ● If the protocol of the backend server is QUIC, the value can only be **UDP_CONNECT**. ● If the protocol of the backend server is UDP, the value can only be **UDP_CONNECT**. ● If the protocol of the backend server is TCP, the value can only be **TCP**, **HTTP**, or **HTTPS**. ● If the protocol of the backend server is HTTP, the value can only be **TCP**, **HTTP**, or **HTTPS**. ● If the protocol of the backend server is HTTPS, the value can only be **TCP**, **HTTP**, or **HTTPS**.
url_path	String	Specifies the HTTP request path for the health check. The value must start with a slash (/), and the default value is **/**. The value can contain letters, digits, hyphens (-), slashes (/), periods (.), percentage signs (%), question marks (?), pound signs (#), ampersand signs (&), and the extended character set: _;~!()*[]@$^:',+. Note: This parameter is available only when **type** is set to **HTTP** or **HTTPS**.

Table 5-684 ConnectionDrain

Parameter	Type	Description
enable	Boolean	Specifies whether to enable **connection_drain**. Value options: • **true**: Enable this option. • **false**: Disable this option. Default value: **true**
timeout	Integer	Specifies the deregistration delay timeout, in seconds. The value ranges from **10** to **4000**.

Table 5-685 QuicCidHashStrategy

Parameter	Type	Description
len	Integer	Specifies the length of the hash factor in the connection ID, in byte. This parameter is valid only when the load balancing algorithm is **QUIC_CID**. Value range: 1 to 20 Default value: 3
offset	Integer	Specifies the start position in the connection ID as the hash factor, in byte. This parameter is valid only when the load balancing algorithm is **QUIC_CID**. Value range: 0 to 19 Default value: 1

Example Requests

```
GET https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/master-slave-pools/36ce7086-a496-4666-9064-5ba0e6840c75
```

Example Responses

Status code: 200

Successful request.

```
{
  "pool" : {
    "lb_algorithm" : "LEAST_CONNECTIONS",
    "type" : "ip",
    "vpc_id" : "3sae7086-a416-4666-9064-5b340e6840125",
    "protocol" : "TCP",
    "description" : "",
```



```
  "loadbalancers" : [ {
    "id" : "098b2f68-af1c-41a9-8efd-69958722af62"
  } ],
  "project_id" : "99a3fff0d03c428eac3678da6a7d0f24",
  "session_persistence" : null,
  "healthmonitor" : {
    "monitor_port" : null,
    "id" : "36ce7086-a496-4666-9064-5ba0e6840c75",
    "domain_name" : "",
    "name" : "My Healthmonitor",
    "max_retries" : 3,
    "max_retries_down" : 3,
    "admin_state_up" : true,
    "type" : "HTTP",
    "timeout" : 30,
    "delay" : 1,
    "http_method" : "get",
    "url_path" : "/",
    "expected_codes" : "200"
  },
  "listeners" : [ {
    "id" : "0b11747a-b139-492f-9692-2df0b1c87193"
  } ],
  "members" : [ {
    "admin_state_up" : true,
    "address" : "172.16.0.210",
    "protocol_port" : 80,
    "id" : "2e7b36d2-66c8-4825-bcd2-211d99978680",
    "operating_status" : "OFFLINE",
    "status" : [ ],
    "instance_id" : "",
    "device_id" : "",
    "device_owner" : "",
    "member_type" : "ip",
    "role" : "master",
    "ip_version" : "v4",
    "name" : "cx-test-master",
    "subnet_cidr_id" : ""
  }, {
    "admin_state_up" : true,
    "address" : "172.16.0.211",
    "protocol_port" : 81,
    "id" : "2e7b36d2-66c8-4823-bsd2-21sa199978681",
    "operating_status" : "OFFLINE",
    "status" : [ ],
    "instance_id" : "",
    "device_id" : "",
    "device_owner" : "",
    "member_type" : "ip",
    "role" : "slave",
    "ip_version" : "v4",
    "name" : "cx-test-slave",
    "subnet_cidr_id" : ""
  } ],
  "id" : "36ce7086-a496-4666-9064-5ba0e6840c75",
  "name" : "My pool",
  "ip_version" : "dualstack",
  "created_at" : "2021-03-26T01:33:12Z",
  "updated_at" : "2021-03-26T01:33:12Z"
 },
 "request_id" : "c1a60da2-1ec7-4a1c-b4cc-73e1a57b368e"
}
```


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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ShowMasterSlavePoolSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowMasterSlavePoolRequest request = new ShowMasterSlavePoolRequest();
        request.withPoolId("{pool_id}");
        try {
            ShowMasterSlavePoolResponse response = client.showMasterSlavePool(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowMasterSlavePoolRequest()
        request.pool_id = "{pool_id}"
        response = client.show_master_slave_pool(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowMasterSlavePoolRequest{}
    request.PoolId = "{pool_id}"
    response, err := client.ShowMasterSlavePool(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	Successful request.

Error Codes

See **Error Codes**.

5.16.4 Deleting an Active/Standby Backend Server Group

Function

This API is used to delete an active/standby backend server group.

Constraints

Deleting an active/standby backend server group will also delete all its backend servers and health checks.

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v3/{project_id}/elb/master-slave-pools/{pool_id}

Table 5-686 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
pool_id	Yes	String	Specifies the ID of the active/standby backend server group.

Request Parameters

Table 5-687 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

None

Example Requests

```
DELETE https://{ELB_Endpoint}/v3/99a3fff0d03c428eac3678da6a7d0f24/elb/master-slave-pools/36ce7086-a496-4666-9064-5ba0e6840c75
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class DeleteMasterSlavePoolSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
```



```
                .build();
        DeleteMasterSlavePoolRequest request = new DeleteMasterSlavePoolRequest();
        request.withPoolId("{pool_id}");
        try {
            DeleteMasterSlavePoolResponse response = client.deleteMasterSlavePool(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteMasterSlavePoolRequest()
        request.pool_id = "{pool_id}"
        response = client.delete_master_slave_pool(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteMasterSlavePoolRequest{}
    request.PoolId = "{pool_id}"
    response, err := client.DeleteMasterSlavePool(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 DELETE requests.

Error Codes

See **Error Codes**.

5.17 Log

5.17.1 Creating a Log

Function

This API is used to create a log.

Calling Method

For details, see **Calling APIs**.

URI

POST /v3/{project_id}/elb/logtanks

Table 5-688 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Request Parameters

Table 5-689 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Table 5-690 Request body parameters

Parameter	Mandatory	Type	Description
logtank	Yes	**CreateLogtankOption** object	Specifies the request parameter for creating a log.

Table 5-691 CreateLogtankOption

Parameter	Mandatory	Type	Description
loadbalancer_id	Yes	String	Specifies the load balancer ID.
log_group_id	Yes	String	Specifies the log group ID. This parameter is available for all services other than ELB.
log_topic_id	Yes	String	Specifies the ID of the log subscription topic. This parameter is available for all services other than ELB.

Response Parameters

Status code: 201

Table 5-692 Response body parameters

Parameter	Type	Description
logtank	**Logtank** object	Provides supplementary information.
request_id	String	Specifies the request ID. Note: The value is automatically generated.

Table 5-693 Logtank

Parameter	Type	Description
id	String	Specifies the log ID.
project_id	String	Specifies the project ID.
loadbalancer_id	String	Specifies the load balancer ID.
log_group_id	String	Specifies the log group ID.
log_topic_id	String	Specifies the log topic ID.

Example Requests

Creating a log for a load balancer

```
POST https://{ELB_Endpoint}/v3/060576798a80d5762fafc01a9b5eedc7/elb/logtanks

{
  "logtank" : {
    "log_topic_id" : "5b9b8370-a1fc-4c59-a509-483a673c8a94",
    "log_group_id" : "7733882e-f7fa-4fb0-a460-0605c48a2280",
    "loadbalancer_id" : "47ecc304-3f1a-4cc6-9c1c-72add483b9ce"
  }
}
```

Example Responses

Status code: 201

Created

```
{
  "request_id" : "c5aea69b657295bef71cd05da2959206",
  "logtank" : {
    "project_id" : "060576798a80d5762fafc01a9b5eedc7",
    "log_topic_id" : "5b9b8370-a1fc-4c59-a509-483a673c8a94",
    "id" : "603e507f-3e18-498b-9460-01a3b6c28fc5",
    "log_group_id" : "7733882e-f7fa-4fb0-a460-0605c48a2280",
    "loadbalancer_id" : "47ecc304-3f1a-4cc6-9c1c-72add483b9ce"
```

```
    }
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Creating a log for a load balancer

```
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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class CreateLogtankSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        CreateLogtankRequest request = new CreateLogtankRequest();
        CreateLogtankRequestBody body = new CreateLogtankRequestBody();
        CreateLogtankOption logtankbody = new CreateLogtankOption();
        logtankbody.withLoadbalancerId("47ecc304-3f1a-4cc6-9c1c-72add483b9ce")
            .withLogGroupId("7733882e-f7fa-4fb0-a460-0605c48a2280")
            .withLogTopicId("5b9b8370-a1fc-4c59-a509-483a673c8a94");
        body.withLogtank(logtankbody);
        request.withBody(body);
        try {
            CreateLogtankResponse response = client.createLogtank(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

Creating a log for a load balancer

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = CreateLogtankRequest()
        logtankbody = CreateLogtankOption(
            loadbalancer_id="47ecc304-3f1a-4cc6-9c1c-72add483b9ce",
            log_group_id="7733882e-f7fa-4fb0-a460-0605c48a2280",
            log_topic_id="5b9b8370-a1fc-4c59-a509-483a673c8a94"
        )
        request.body = CreateLogtankRequestBody(
            logtank=logtankbody
        )
        response = client.create_logtank(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

Creating a log for a load balancer

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateLogtankRequest{}
    logtankbody := &model.CreateLogtankOption{
        LoadbalancerId: "47ecc304-3f1a-4cc6-9c1c-72add483b9ce",
        LogGroupId: "7733882e-f7fa-4fb0-a460-0605c48a2280",
        LogTopicId: "5b9b8370-a1fc-4c59-a509-483a673c8a94",
    }
    request.Body = &model.CreateLogtankRequestBody{
        Logtank: logtankbody,
    }
    response, err := client.CreateLogtank(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**.

5.17.2 Querying Logs

Function

This API is used to query logs.

Constraints

This API has the following constraints:

- Parameters **marker**, **limit**, and **page_reverse** are used for pagination query.
- Parameters **marker** and **page_reverse** take effect only when they are used together with parameter **limit**.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/logtanks

Table 5-694 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Table 5-695 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Specifies the number of records on each page. Value range: 0–2000 Default value: 2000
marker	No	String	Specifies the ID of the last record on the previous page. Note: • This parameter must be used together with **limit**. • If this parameter is not specified, the first page will be queried. • This parameter cannot be left blank or set to an invalid ID.

Parameter	Mandatory	Type	Description
page_reverse	No	Boolean	Specifies whether to use reverse query. Value options: • **true**: Query the previous page. • **false** (default): Query the next page. Note: • This parameter must be used together with **limit**. • If **page_reverse** is set to **true** and you want to query the previous page, set the value of **marker** to the value of **previous_marker**.
enterprise_project_id	No	Array of strings	Specifies the ID of the enterprise project. • If **enterprise_project_id** is not specified, resources in all enterprise projects are queried by default. Fine-grained authorization is performed. The **elb:logtanks:list** permission must be assigned to the user group. • If **enterprise_project_id** is specified, the value can be a specific enterprise project ID or **all_granted_eps**. If the value is a specific enterprise project ID, only resources in the enterprise project are queried. If the value is **all_granted_eps**, resources in the enterprise projects with the **elb:logtanks:list** permission are queried. Multiple values can be queried in the format of *enterprise_project_id=xxx&enterprise_project_id=xxx*.

Parameter	Mandatory	Type	Description
id	No	Array of strings	Specifies the ID of the log tank. Multiple IDs can be queried in the format of *id=xxx&id=xxx*.
loadbalancer_id	No	Array of strings	Specifies the ID of a load balancer. Multiple IDs can be queried in the format of *loadbalancer_id=xxx&loadbalancer_id=xxx*.
log_group_id	No	Array of strings	Specifies the log group ID. Multiple IDs can be queried in the format of *log_group_id=xxx&log_group_id=xxx*.
log_topic_id	No	Array of strings	Specifies the log topic ID. Multiple IDs can be queried in the format of *log_topic_id=xxx&log_topic_id=xxx*.

Request Parameters

Table 5-696 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-697 Response body parameters

Parameter	Type	Description
logtanks	Array of **Logtank** objects	Provides supplementary information.
page_info	**PageInfo** object	Specifies pagination information about the load balancer.

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.

Table 5-698 Logtank

Parameter	Type	Description
id	String	Specifies the log ID.
project_id	String	Specifies the project ID.
loadbalancer_id	String	Specifies the load balancer ID.
log_group_id	String	Specifies the log group ID.
log_topic_id	String	Specifies the log topic ID.

Table 5-699 PageInfo

Parameter	Type	Description
previous_marker	String	Specifies the ID of the first record in the pagination query result. When **page_reverse** is set to **true**, this parameter is used together to query resources on the previous page.
next_marker	String	Specifies the ID of the last record in the pagination query result.
current_count	Integer	Specifies the number of records.

Example Requests

Querying logs of multiple load balancers

```
GET https://{ELB_Endpoint}/v3/060576798a80d5762fafc01a9b5eedc7/elb/logtanks?
loadbalancer_id=995b98d7-6010-4502-a91a-756f399088f8&loadbalancer_id=37e9c3e3-08a2-48e9-
acee-431159a33cc2
```

Example Responses

Status code: 200

OK

```
{
  "request_id" : "5b43d31cd5217ffca57c2c4177e1b1ee",
  "logtanks" : [ {
```



```
    "project_id" : "060576798a80d5762fafc01a9b5eedc7",
    "log_topic_id" : "5b9b8370-a1fc-4c59-a509-483a673c8a94",
    "id" : "281e8768-94f9-45e9-9f3d-9fe2a122ad67",
    "log_group_id" : "7733882e-f7fa-4fb0-a460-0605c48a2280",
    "loadbalancer_id" : "995b98d7-6010-4502-a91a-756f399088f8"
  } ],
  "page_info" : {
    "next_marker" : "281e8768-94f9-45e9-9f3d-9fe2a122ad67",
    "previous_marker" : "281e8768-94f9-45e9-9f3d-9fe2a122ad67",
    "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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ListLogtanksSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ListLogtanksRequest request = new ListLogtanksRequest();
        try {
            ListLogtanksResponse response = client.listLogtanks(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListLogtanksRequest()
        response = client.list_logtanks(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
```



```
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListLogtanksRequest{}
    response, err := client.ListLogtanks(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**.

5.17.3 Viewing the Details of a Log

Function

This API is used to view the details of a log.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/logtanks/{logtank_id}

Table 5-700 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
logtank_id	Yes	String	Specifies the log ID.

Request Parameters

Table 5-701 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

Status code: 200

Table 5-702 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
logtank	**Logtank** object	Provides supplementary information.

Table 5-703 Logtank

Parameter	Type	Description
id	String	Specifies the log ID.
project_id	String	Specifies the project ID.
loadbalancer_id	String	Specifies the load balancer ID.
log_group_id	String	Specifies the log group ID.
log_topic_id	String	Specifies the log topic ID.

Example Requests

Viewing the details of a log

```
GET https://{ELB_Endpoint}/v3/060576798a80d5762fafc01a9b5eedc7/elb/logtanks/603e507f-3e18-498b-9460-01a3b6c28fc5
```

Example Responses

Status code: 200

OK

```
{
  "logtank" : {
```



```
    "project_id" : "060576798a80d5762fafc01a9b5eedc7",
    "log_topic_id" : "5b9b8370-a1fc-4c59-a509-483a673c8a94",
    "id" : "603e507f-3e18-498b-9460-01a3b6c28fc5",
    "log_group_id" : "7733882e-f7fa-4fb0-a460-0605c48a2280",
    "loadbalancer_id" : "47ecc304-3f1a-4cc6-9c1c-72add483b9ce"
  },
  "request_id" : "59662f86620f8fc09c908eed060a2f0e"
}
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ShowLogtankSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowLogtankRequest request = new ShowLogtankRequest();
        request.withLogtankId("{logtank_id}");
        try {
            ShowLogtankResponse response = client.showLogtank(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowLogtankRequest()
        request.logtank_id = "{logtank_id}"
        response = client.show_logtank(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
```



```
        WithCredential(auth).
        Build())

    request := &model.ShowLogtankRequest{}
    request.LogtankId = "{logtank_id}"
    response, err := client.ShowLogtank(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**.

5.17.4 Updating a Log

Function

This API is used to update a log.

Calling Method

For details, see **Calling APIs**.

URI

PUT /v3/{project_id}/elb/logtanks/{logtank_id}

Table 5-704 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
logtank_id	Yes	String	Specifies the log ID.

Request Parameters

Table 5-705 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Table 5-706 Request body parameters

Parameter	Mandatory	Type	Description
logtank	Yes	**UpdateLogtankOption** object	Specifies the request parameter for updating a log.

Table 5-707 UpdateLogtankOption

Parameter	Mandatory	Type	Description
log_group_id	No	String	Specifies the log group ID. This parameter is available for all services other than ELB.
log_topic_id	No	String	Specifies the ID of the log subscription topic. This parameter is available for all services other than ELB.

Response Parameters

Status code: 200

Table 5-708 Response body parameters

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.
logtank	**Logtank** object	Specifies the log details.

Table 5-709 Logtank

Parameter	Type	Description
id	String	Specifies the log ID.
project_id	String	Specifies the project ID.
loadbalancer_id	String	Specifies the load balancer ID.
log_group_id	String	Specifies the log group ID.
log_topic_id	String	Specifies the log topic ID.

Example Requests

Updating a log

```
PUT https://{ELB_Endpoint}/v3/060576798a80d5762fafc01a9b5eedc7/elb/logtanks/
603e507f-3e18-498b-9460-01a3b6c28fc5

{
  "logtank" : {
    "log_topic_id" : "5b9b8370-a1fc-4c59-a509-483a673c8a94",
    "log_group_id" : "7733882e-f7fa-4fb0-a460-0605c48a2280"
  }
}
```

Example Responses

Status code: 200

OK

```
{
  "logtank" : {
    "project_id" : "060576798a80d5762fafc01a9b5eedc7",
    "log_topic_id" : "5b9b8370-a1fc-4c59-a509-483a673c8a94",
    "id" : "603e507f-3e18-498b-9460-01a3b6c28fc5",
    "log_group_id" : "7733882e-f7fa-4fb0-a460-0605c48a2280",
    "loadbalancer_id" : "47ecc304-3f1a-4cc6-9c1c-72add483b9ce"
  },
  "request_id" : "59662f86620f8fc09c908eed060a2f0e"
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Updating a log

```
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.elb.v3.region.ElbRegion;
```



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


public class UpdateLogtankSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        UpdateLogtankRequest request = new UpdateLogtankRequest();
        request.withLogtankId("{logtank_id}");
        UpdateLogtankRequestBody body = new UpdateLogtankRequestBody();
        UpdateLogtankOption logtankbody = new UpdateLogtankOption();
        logtankbody.withLogGroupId("7733882e-f7fa-4fb0-a460-0605c48a2280")
            .withLogTopicId("5b9b8370-a1fc-4c59-a509-483a673c8a94");
        body.withLogtank(logtankbody);
        request.withBody(body);
        try {
            UpdateLogtankResponse response = client.updateLogtank(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

Updating a log

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = UpdateLogtankRequest()
        request.logtank_id = "{logtank_id}"
        logtankbody = UpdateLogtankOption(
            log_group_id="7733882e-f7fa-4fb0-a460-0605c48a2280",
            log_topic_id="5b9b8370-a1fc-4c59-a509-483a673c8a94"
        )
        request.body = UpdateLogtankRequestBody(
            logtank=logtankbody
        )
        response = client.update_logtank(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

Updating a log

```
package main

import (
    "fmt"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/core/auth/basic"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.UpdateLogtankRequest{}
    request.LogtankId = "{logtank_id}"
    logGroupIdLogtank:= "7733882e-f7fa-4fb0-a460-0605c48a2280"
    logTopicIdLogtank:= "5b9b8370-a1fc-4c59-a509-483a673c8a94"
    logtankbody := &model.UpdateLogtankOption{
```

```
        LogGroupId: &logGroupIdLogtank,
        LogTopicId: &logTopicIdLogtank,
    }
    request.Body = &model.UpdateLogtankRequestBody{
        Logtank: logtankbody,
    }
    response, err := client.UpdateLogtank(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**.

5.17.5 Deleting a Log

Function

This API is used to delete a log.

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v3/{project_id}/elb/logtanks/{logtank_id}

Table 5-710 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
logtank_id	Yes	String	Specifies the log ID.

Request Parameters

Table 5-711 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the token used for IAM authentication.

Response Parameters

None

Example Requests

Deleting a log

```
DELETE https://{ELB_Endpoint}/v3/060576798a80d5762fafc01a9b5eedc7/elb/logtanks/
603e507f-3e18-498b-9460-01a3b6c28fc5
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class DeleteLogtankSolution {

    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);
```



```
        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        DeleteLogtankRequest request = new DeleteLogtankRequest();
        request.withLogtankId("{logtank_id}");
        try {
            DeleteLogtankResponse response = client.deleteLogtank(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = DeleteLogtankRequest()
        request.logtank_id = "{logtank_id}"
        response = client.delete_logtank(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
```

```
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeleteLogtankRequest{}
    request.LogtankId = "{logtank_id}"
    response, err := client.DeleteLogtank(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**.

5.18 Asynchronous Task

5.18.1 Querying the Asynchronous Tasks

Function

This API is used to query the status of an asynchronous task like exporting, copying, or upgrading load balancers.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/jobs

Table 5-712 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Table 5-713 Query Parameters

Parameter	Mandatory	Type	Description
job_id	No	String	Specifies the task ID.
job_type	No	String	Specifies the task type.
status	No	String	Specifies the task status. Value range: **INIT**, **RUNNING**, **FAIL**, **SUCCESS**, **ROLLBACKING**, **COMPLETE**, **ROLLBACK_FAIL**, and **CANCEL**.
error_code	No	String	Specifies the error code of the task.
resource_id	No	String	Specifies the resource ID.
project_id	No	String	Specifies the project ID.
begin_time	No	String	Specifies the time when the task started, in the format of *yyyy-MM-dd'T'HH:mm:ss*. The tasks that started on or after the specified time will be returned.

Request Parameters

None

Response Parameters

Status code: 200

Table 5-714 Response body parameters

Parameter	Type	Description
jobs	Array of **MainJob** objects	Specifies the task list.
request_id	String	Specifies the request ID. Note: The value is automatically generated.

Table 5-715 MainJob

Parameter	Type	Description
status	String	Specifies the task status.
begin_time	String	Specifies the time when the task was started.
end_time	String	Specifies the time when the task was ended.
job_id	String	Specifies the task ID.
job_type	String	Specifies the task type.
error_code	String	Specifies the task error code.
error_msg	String	Specifies the task error message.
project_id	String	Specifies the project ID.
resource_id	String	Specifies the resource ID.
sub_jobs	Array of **SubJob** objects	Specifies the subtask list.

Table 5-716 SubJob

Parameter	Type	Description
status	String	Specifies the task status.

Parameter	Type	Description
begin_time	String	Specifies the time when the task was started.
end_time	String	Specifies the time when the task was ended.
job_id	String	Specifies the task ID.
job_type	String	Specifies the task type.
error_code	String	Specifies the task error code.
error_msg	String	Specifies the task error message.
project_id	String	Specifies the project ID.
resource_id	String	Specifies the resource ID.
entities	Array of **JobEntities** objects	Specifies the resource to be processed in a subtask.

Table 5-717 JobEntities

Parameter	Type	Description
resource_id	String	Specifies the ID of the resource associated with a subtask.
resource_type	String	Specifies the type of the resource associated with a subtask.

Example Requests

https://elb.cn-southwest-242.myhuaweicloud.com/v3/7b7705dce1e847b08b3b16dda67fec24/elb/jobs


```
{
  "request_id" : "029f8cca-4d92-4b3e-9370-b36d382f969b",
  "jobs" : [ {
    "status" : "COMPLETE",
    "begin_time" : "2024-03-23T08:20:42Z",
    "end_time" : "2024-03-23T08:49:11Z",
    "job_id" : "ef6da45b-35d9-4c18-8c35-0b80d94ab9e6",
    "resource_id" : "9f5b432c-987e-4777-a1bc-6642be4b2b50",
    "job_type" : "UPGRADE",
    "error_code" : "",
    "error_msg" : "",
    "project_id" : "7b7705dce1e847b08b3b16dda67fec24",
    "sub_jobs" : [ {
      "status" : "SUCCESS",
      "entities" : [ {
        "resource_id" : "9f5b432c-987e-4777-a1bc-6642be4b2b50",
        "resource_type" : "loadbalancer"
      } ],
      "begin_time" : "2024-03-23T08:47:11Z",
      "end_time" : "2024-03-23T08:47:11Z",
```



```
    "job_id" : "481a5ab3-b3ff-46fa-b074-d3b8e09ab9cb",
    "resource_id" : "9f5b432c-987e-4777-a1bc-6642be4b2b50",
    "job_type" : "UPGRADE_TRAFFIC_SWITCH",
    "error_code" : "",
    "error_msg" : "",
    "project_id" : "7b7705dce1e847b08b3b16dda67fec24"
   }, {
    "status" : "SUCCESS",
    "entities" : [ {
     "resource_id" : "9f5b432c-987e-4777-a1bc-6642be4b2b50",
     "resource_type" : "loadbalancer"
    } ],
    "begin_time" : "2024-03-23T08:20:42Z",
    "end_time" : "2024-03-23T08:46:44Z",
    "job_id" : "c4cf4e5b-fa53-427d-ad43-497e7a876c2e",
    "resource_id" : "9f5b432c-987e-4777-a1bc-6642be4b2b50",
    "job_type" : "UPGRADE_INIT",
    "error_code" : "",
    "error_msg" : "",
    "project_id" : "7b7705dce1e847b08b3b16dda67fec24"
   }, {
    "status" : "SUCCESS",
    "entities" : [ {
     "resource_id" : "9f5b432c-987e-4777-a1bc-6642be4b2b50",
     "resource_type" : "loadbalancer"
    } ],
    "begin_time" : "2024-03-23T08:49:11Z",
    "end_time" : "2024-03-23T08:49:11Z",
    "job_id" : "ee56e027-5d52-4bd9-abba-9821a742a466",
    "resource_id" : "9f5b432c-987e-4777-a1bc-6642be4b2b50",
    "job_type" : "UPGRADE_COMPLETE",
    "error_code" : "",
    "error_msg" : "",
    "project_id" : "7b7705dce1e847b08b3b16dda67fec24"
   } ]
  } ],
  "page_info" : {
   "previous_marker" : "ef6da45b-35d9-4c18-8c35-0b80d94ab9e6",
   "current_count" : 1
  }
}
```


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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ListJobsSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ListJobsRequest request = new ListJobsRequest();
        try {
            ListJobsResponse response = client.listJobs(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListJobsRequest()
        response = client.list_jobs(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListJobsRequest{}
    response, err := client.ListJobs(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	Query succeeded.

Error Codes

See **Error Codes**.

5.19 Feature Configuration

5.19.1 Querying the Feature Configurations of ELB

Function

This API is used to query the feature configurations of ELB of a tenant.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/feature/configs

Table 5-718 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Table 5-719 Query Parameters

Parameter	Mandatory	Type	Description
feature	No	String	Specifies the feature name.

Request Parameters

None

Response Parameters

Status code: 200

Table 5-720 Response body parameters

Parameter	Type	Description
configs	Array of **FeatureConfig** objects	Specifies the feature configuration list.
page_info	**PageInfo** object	Specifies the specification pagination information.

Parameter	Type	Description
request_id	String	Specifies the request ID. Note: The value is automatically generated.

Table 5-721 FeatureConfig

Parameter	Type	Description
id	String	Specifies the ID of the configuration.
created_at	String	Specifies the creation time.
updated_at	String	Specifies the update time.
service	String	Specifies the service. The value is fixed at **ELB**.
tenant_id	String	Specifies the tenant ID, which has the same meaning as that of **project_id**.
feature	String	Specifies the feature name.
switch	Boolean	Specifies whether to enable feature configuration. Value options: • **true**: The feature configuration has taken effect. • **false**: The feature configuration does not take effect.
type	String	Specifies the type of the feature configuration value. For example, **INT** indicates an integer.
value	String	Specifies the feature configuration value. For example, the value **true** or **false** indicates that the feature is enabled or disabled. The feature value of the quota is an integer, indicating that the quota is limited.
description	String	Specifies the feature configuration description.
caller	String	Specifies the configuration creator.

Table 5-722 PageInfo

Parameter	Type	Description
previous_marker	String	Specifies the ID of the first record in the pagination query result. When **page_reverse** is set to **true**, this parameter is used together to query resources on the previous page.
next_marker	String	Specifies the ID of the last record in the pagination query result.
current_count	Integer	Specifies the number of records.

Example Requests

```
https://{ELB_Endpoint}/v3/7b7705dce1e847b08b3b16dda67fec24/elb/feature/configs
```

Example Responses

Status code: 200

Query succeeded.

```
{
  "request_id" : "7d7874c9-9296-4337-bd97-93d69619f38e",
  "configs" : [ {
    "created_at" : "2024-05-16T12:54:54Z",
    "updated_at" : "2024-05-16T12:54:54Z",
    "id" : "1911170d-27b0-4609-9ccd-f67fc3359092",
    "service" : "ELB",
    "tenant_id" : "0c1503d710984bad92306faea3654dfd",
    "feature" : "feature.gates.batch_create_v2_loadbalancers_amount",
    "switch" : true,
    "type" : "INT",
    "value" : "10",
    "description" : "",
    "caller" : "unknown"
  } ],
  "page_info" : {
    "previous_marker" : "1911170d-27b0-4609-9ccd-f67fc3359092",
    "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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
```



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


public class ListFeatureConfigsSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ListFeatureConfigsRequest request = new ListFeatureConfigsRequest();
        try {
            ListFeatureConfigsResponse response = client.listFeatureConfigs(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()
```



```
    try:
        request = ListFeatureConfigsRequest()
        response = client.list_feature_configs(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListFeatureConfigsRequest{}
    response, err := client.ListFeatureConfigs(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	Query succeeded.

Error Codes

See **Error Codes**.

5.19.2 Querying the Feature Configurations of a Load Balancer

Function

This API is used to query the feature configurations of a load balancer.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}/features

Table 5-723 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
loadbalancer_id	Yes	String	Specifies the load balancer ID.

Request Parameters

None

Response Parameters

Status code: 200

Table 5-724 Response body parameters

Parameter	Type	Description
features	Array of **LoadbalancerFeature** objects	Specifies the load balancer feature information list.
request_id	String	Specifies the request ID. Note: The value is automatically generated.

Table 5-725 LoadbalancerFeature

Parameter	Type	Description
feature	String	Specifies the feature name.
type	String	Specifies the type of the feature configuration value. For example, **INT** indicates an integer.
value	String	Specifies the feature value. For example, the value **true** or **false** indicates that the feature is enabled or disabled. The feature value of the quota is an integer, indicating that the quota is limited.

Example Requests

```
https://elb.cn-southwest-242.myhuaweicloud.com/v3/0c1503d710984bad92306faea3654dfd/elb/loadbalancers/6c9ddefb-c0c2-40fb-9505-0b4c81fac234/features
```

Example Responses

Status code: 200

Query succeeded.

```
{
  "features" : [ {
    "feature" : "update_elastic_flavor",
    "value" : "true",
    "type" : "BOOL"
  }, {
    "feature" : "tcpssl",
    "value" : "true",
    "type" : "BOOL"
  }, {
    "feature" : "dnat_forward_mode_enable",
    "value" : "true",
    "type" : "BOOL"
  }, {
    "feature" : "upgrade_l4_resource_package",
    "value" : "false",
    "type" : "BOOL"
  }, {
    "feature" : "upgrade_l7_resource_package",
    "value" : "false",
    "type" : "BOOL"
  }, {
    "feature" : "l7policy_cors",
    "value" : "true",
    "type" : "BOOL"
  }, {
    "feature" : "l7policy_traffic_limit",
    "value" : "true",
    "type" : "BOOL"
  }, {
    "feature" : "listener_qos",
    "value" : "true",
    "type" : "BOOL"
  }, {
```



```
    "feature" : "l7_traffic_mirror",
    "value" : "true",
    "type" : "BOOL"
  }, {
    "feature" : "traffic_mirror_enable",
    "value" : "true",
    "type" : "BOOL"
  }, {
    "feature" : "nat64_enable",
    "value" : "true",
    "type" : "BOOL"
  }, {
    "feature" : "multi_eip",
    "value" : "true",
    "type" : "BOOL"
  }, {
    "feature" : "multi_vip",
    "value" : "true",
    "type" : "BOOL"
  } ],
  "request_id" : "d8e8d908-1f54-46da-b254-45203bc1115d"
}
```

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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ListLoadbalancerFeatureSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ListLoadbalancerFeatureRequest request = new ListLoadbalancerFeatureRequest();
        request.withLoadbalancerId("{loadbalancer_id}");
        try {
            ListLoadbalancerFeatureResponse response = client.listLoadbalancerFeature(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ListLoadbalancerFeatureRequest()
        request.loadbalancer_id = "{loadbalancer_id}"
        response = client.list_loadbalancer_feature(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ListLoadbalancerFeatureRequest{}
    request.LoadbalancerId = "{loadbalancer_id}"
    response, err := client.ListLoadbalancerFeature(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	Query succeeded.

Error Codes

See **Error Codes**.

5.20 Asynchronous Tasks

5.20.1 Querying the Status of an Asynchronous Task

Function

This API is used to query the status of an asynchronous task like importing, copying, or upgrading load balancers.

Calling Method

For details, see **Calling APIs**.

URI

GET /v3/{project_id}/elb/jobs/{job_id}

Table 5-726 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
job_id	Yes	String	Specifies the task ID.

Request Parameters

None

Response Parameters

Status code: 200

Table 5-727 Response body parameters

Parameter	Type	Description
job	**MainJob** object	Specifies the response body for querying asynchronous tasks such as copy tasks.
request_id	String	Specifies the request ID. Note: The value is automatically generated.

Table 5-728 MainJob

Parameter	Type	Description
status	String	Specifies the task status.
begin_time	String	Specifies the time when the task was started.
end_time	String	Specifies the time when the task was ended.
job_id	String	Specifies the task ID.
job_type	String	Specifies the task type.
error_code	String	Specifies the task error code.
error_msg	String	Specifies the task error message.

Parameter	Type	Description
project_id	String	Specifies the project ID.
resource_id	String	Specifies the resource ID.
sub_jobs	Array of **SubJob** objects	Specifies the subtask list.

Table 5-729 SubJob

Parameter	Type	Description
status	String	Specifies the task status.
begin_time	String	Specifies the time when the task was started.
end_time	String	Specifies the time when the task was ended.
job_id	String	Specifies the task ID.
job_type	String	Specifies the task type.
error_code	String	Specifies the task error code.
error_msg	String	Specifies the task error message.
project_id	String	Specifies the project ID.
resource_id	String	Specifies the resource ID.
entities	Array of **JobEntities** objects	Specifies the resource to be processed in a subtask.

Table 5-730 JobEntities

Parameter	Type	Description
resource_id	String	Specifies the ID of the resource associated with a subtask.
resource_type	String	Specifies the type of the resource associated with a subtask.

Example Requests

```
https://elb.cn-southwest-242.myhuaweicloud.com/v3/7b7705dce1e847b08b3b16dda67fec24/elb/jobs/37d5c1fd-fa57-4c6d-bdcd-d523095c05e8

{
```



```
"job" : {
  "status" : "COMPLETE",
  "begin_time" : "2024-03-23T08:20:42Z",
  "end_time" : "2024-03-23T08:49:11Z",
  "job_id" : "ef6da45b-35d9-4c18-8c35-0b80d94ab9e6",
  "resource_id" : "9f5b432c-987e-4777-a1bc-6642be4b2b50",
  "job_type" : "UPGRADE",
  "error_code" : "",
  "error_msg" : "",
  "project_id" : "7b7705dce1e847b08b3b16dda67fec24",
  "sub_jobs" : [ {
    "status" : "SUCCESS",
    "entities" : [ {
      "resource_id" : "9f5b432c-987e-4777-a1bc-6642be4b2b50",
      "resource_type" : "loadbalancer"
    } ],
    "begin_time" : "2024-03-23T08:47:11Z",
    "end_time" : "2024-03-23T08:47:11Z",
    "job_id" : "481a5ab3-b3ff-46fa-b074-d3b8e09ab9cb",
    "resource_id" : "9f5b432c-987e-4777-a1bc-6642be4b2b50",
    "job_type" : "UPGRADE_TRAFFIC_SWITCH",
    "error_code" : "",
    "error_msg" : "",
    "project_id" : "7b7705dce1e847b08b3b16dda67fec24"
  }, {
    "status" : "SUCCESS",
    "entities" : [ {
      "resource_id" : "9f5b432c-987e-4777-a1bc-6642be4b2b50",
      "resource_type" : "loadbalancer"
    } ],
    "begin_time" : "2024-03-23T08:20:42Z",
    "end_time" : "2024-03-23T08:46:44Z",
    "job_id" : "c4cf4e5b-fa53-427d-ad43-497e7a876c2e",
    "resource_id" : "9f5b432c-987e-4777-a1bc-6642be4b2b50",
    "job_type" : "UPGRADE_INIT",
    "error_code" : "",
    "error_msg" : "",
    "project_id" : "7b7705dce1e847b08b3b16dda67fec24"
  }, {
    "status" : "SUCCESS",
    "entities" : [ {
      "resource_id" : "9f5b432c-987e-4777-a1bc-6642be4b2b50",
      "resource_type" : "loadbalancer"
    } ],
    "begin_time" : "2024-03-23T08:49:11Z",
    "end_time" : "2024-03-23T08:49:11Z",
    "job_id" : "ee56e027-5d52-4bd9-abba-9821a742a466",
    "resource_id" : "9f5b432c-987e-4777-a1bc-6642be4b2b50",
    "job_type" : "UPGRADE_COMPLETE",
    "error_code" : "",
    "error_msg" : "",
    "project_id" : "7b7705dce1e847b08b3b16dda67fec24"
  } ]
},
"request_id" : "39551f69-3c49-4200-8ad3-73f9a8b4a3e4"
}
```


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.elb.v3.region.ElbRegion;
import com.huaweicloud.sdk.elb.v3.*;
import com.huaweicloud.sdk.elb.v3.model.*;


public class ShowJobSolution {

    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);

        ElbClient client = ElbClient.newBuilder()
                .withCredential(auth)
                .withRegion(ElbRegion.valueOf("<YOUR REGION>"))
                .build();
        ShowJobRequest request = new ShowJobRequest();
        request.withJobId("{job_id}");
        try {
            ShowJobResponse response = client.showJob(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 huaweicloudsdkelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkelb.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 = ElbClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(ElbRegion.value_of("<YOUR REGION>")) \
        .build()

    try:
        request = ShowJobRequest()
        request.job_id = "{job_id}"
        response = client.show_job(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"
    elb "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3"
    "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/v3/model"
    region "github.com/huaweicloud/huaweicloud-sdk-go-v3/services/elb/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 := elb.NewElbClient(
        elb.ElbClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowJobRequest{}
    request.JobId = "{job_id}"
    response, err := client.ShowJob(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	Query succeeded.

Error Codes

See **Error Codes**.

6 APIs (V2)

6.1 Load Balancer

6.1.1 Creating a Load Balancer

Function

This API is used to create a private network load balancer. After the load balancer is created, its details, such as load balancer ID, IP address, and subnet ID, are returned.

To create a public network load balancer, you also need to call the API for assigning an EIP and associate this IP address to the port bound to the IP address of the private network load balancer.

You can set the **enterprise_project_id** parameter to perform fine-grained authorization for resources.

URI

POST /v2/{project_id}/elb/loadbalancers

Table 6-1 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Request

Table 6-2 Parameter description

Parameter	Mandatory	Type	Description
loadbalancer	Yes	**Loadbalancer** object	Specifies the load balancer. For details, see **Table 6-3**.

Table 6-3 loadbalancer parameter description

Parameter	Mandatory	Type	Description
name	No	String	Specifies the load balancer name. The value contains a maximum of 255 characters.
description	No	String	Provides supplementary information about the load balancer. The value contains a maximum of 255 characters.
tenant_id	No	String	Specifies the ID of the project where the load balancer is used. The value contains a maximum of 255 characters. The value must be the same as the value of **project_id** in the token.
vip_subnet_id	Yes	String	Specifies the ID of the IPv4 subnet where the load balancer works. Obtain the value by listing the subnets (The parameter is **neutron_subnet_id**). The private IP address of the load balancer is in this subnet. Only IPv4 subnets are supported.
provider	No	String	Specifies the provider of the load balancer. The value can only be **vlb**.

Parameter	Mandatory	Type	Description
vip_address	No	String	Specifies the private IP address of the load balancer. This IP address must be the one in the subnet specified by **vip_subnet_id**. If this parameter is not specified, an IP address is automatically assigned to the load balancer from the subnet specified by **vip_subnet_id**. The value contains a maximum of 64 characters. You cannot specify a private IP address for a yearly/monthly load balancer. The system will assign one from the subnet.
admin_state_up	No	Boolean	Specifies the administrative status of the load balancer. The load balancer stops receiving traffic after it is disabled. The value can be one of the following: **true**: Enable the load balancer. **false**: Disable the load balancer. Default value: **true**
enterprise_project_id	No	String	Specifies the enterprise project ID. When creating a load balancer, you can assign an enterprise project to the load balancer. The value is character string **0** or a UUID with hyphens (-). Value **0** indicates the default enterprise project. The default value is **0**. **NOTE** For more information about enterprise projects and how to obtain enterprise project IDs, see **Enterprise Management User Guide**.
protection_status	No	String	Specifies whether modification protection is enabled. The value can be one of the following: • **nonProtection** (default): Modification protection is not enabled. • **consoleProtection**: Modification protection is enabled to avoid that resources are modified by accident on the console.

Parameter	Mandatory	Type	Description
protection_reason	No	String	Specifies the reason to enable modification protection. This parameter is valid only when **protection_status** is set to **consoleProtection**.

Response

Table 6-4 Parameter description

Parameter	Type	Description
loadbalancer	**Loadbalancer** object	Specifies the load balancer. For details, see **Table 6-5**.

Table 6-5 loadbalancer parameter description

Parameter	Type	Description
id	String	Specifies the load balancer ID.
project_id	String	Specifies the ID of the project where the load balancer is used.
tenant_id	String	Specifies the tenant ID.
name	String	Specifies the load balancer name. The value contains a maximum of 255 characters.
description	String	Provides supplementary information about the load balancer. The value contains a maximum of 255 characters.
vip_subnet_id	String	Specifies the ID of the IPv4 subnet where the load balancer works.
vip_port_id	String	Specifies the ID of the port bound to the private IP address of the load balancer.
provider	String	Specifies the provider of the load balancer.

Parameter	Type	Description
vip_address	String	Specifies the private IP address of the load balancer. The value contains a maximum of 64 characters.
listeners	Array of **Listeners** objects	Lists the IDs of listeners added to the load balancer. For details, see **Table 6-6**.
pools	Array of **Pools** objects	Lists the IDs of backend server groups associated with the load balancer. For details, see **Table 6-7**.
operating_status	String	Specifies the operating status of the load balancer. The value can be **ONLINE** or **FROZEN**.
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the load balancer.
admin_state_up	Boolean	Specifies the administrative status of the load balancer. The load balancer stops receiving traffic after it is disabled. Value options: **true**: Enable a load balancer. **false**: Disable the load balancer.
tags	Array	Lists load balancer tags.
created_at	String	Specifies the time when the load balancer was created. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format. The value contains a maximum of 19 characters.
updated_at	String	Specifies the time when the load balancer was updated. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format. The value contains a maximum of 19 characters.

Parameter	Type	Description
enterprise_project_id	String	Specifies the enterprise project ID. When creating a load balancer, you can assign an enterprise project to the load balancer. The value is character string **0** or a UUID with hyphens (-). Value **0** indicates the default enterprise project. **NOTE** For more information about enterprise projects and how to obtain enterprise project IDs, see **Enterprise Management User Guide**.
charge_mode	String	Specifies how the load balancer will be billed. The value can be one of the following: • **flavor**: indicates the guaranteed performance that allows the load balancer to handle up to 50,000 concurrent connections, 5,000 connections and 5,000 queries per second. You will be charged if the load balancer provides guaranteed performance. • **null**: indicates that guaranteed performance is not provided.
billing_info	String	Specifies whether the billing information is left blank.

Parameter	Type	Description
frozen_scene	String	Specifies the scenario where the load balancer is frozen. If there are multiple scenarios, separate them with commas (,). The value can be one of the following: • **POLICE**: The load balancer is frozen for public security. • **ILLEGAL**: The load balancer is frozen due to violation of laws and regulations. • **VERIFY**: The load balancer is frozen because the user fails to pass real-name authentication. • **PARTNER**: The load balancer is frozen by the partner. • **REAR**: Your account is in arrears.
protection_status	String	Specifies whether modification protection is enabled. The value can be one of the following: • **nonProtection** (default): Modification protection is not enabled. • **consoleProtection**: Modification protection is enabled to avoid that resources are modified by accident on the console.
protection_reason	String	Specifies the reason to enable modification protection. This parameter is valid only when **protection_status** is set to **consoleProtection**.
publicips	Array of **PublicIpInfo** objects	Specifies the EIP bound to the load balancer. Only one EIP can be bound to a load balancer.

Table 6-6 listeners parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated listener.

Table 6-7 pools parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated backend server group.

Table 6-8 PublicIpInfo

Parameter	Type	Description
publicip_id	String	Specifies the EIP ID.
publicip_address	String	Specifies the public IP address.
ip_version	Integer	Specifies the IP version. The value can be **4** (IPv4) or **6** (IPv6).

Example Request

- Example request 1: Creating a private network load balancer

```
POST https://{Endpoint}/v2/1867112d054b427e808cc6096d8193a1/elb/loadbalancers

{
    "loadbalancer": {
        "name": "loadbalancer1",
        "description": "simple lb",
        "tenant_id": "1867112d054b427e808cc6096d8193a1",
        "vip_subnet_id": "58077bdb-d470-424b-8c45-2e3c65060a5b",
        "vip_address": "10.0.0.4",
        "admin_state_up": true,
        "enterprise_project_id": "0aad99bc-f5f6-4f78-8404-c598d76b0ed2"
    }
}
```

Example Response

- Example response 1

```
{
    "loadbalancer": {
        "description": "",
        "admin_state_up": true,
        "tenant_id": "1867112d054b427e808cc6096d8193a1",
        "project_id": "1867112d054b427e808cc6096d8193a1",
        "provisioning_status": "ACTIVE",
        "vip_subnet_id": "58077bdb-d470-424b-8c45-2e3c65060a5b",
        "listeners": [],
        "vip_address": "10.0.0.4",
        "vip_port_id": "519f6af5-74aa-4347-9dba-84c440192877",
        "provider": "vlb",
        "pools": [],
        "tags": [],
        "id": "b0657373-0c68-41d1-980f-1a44d9e3ff01",
        "operating_status": "ONLINE",
        "name": "loadbalancer1",
        "created_at": "2018-07-25T01:54:13",
        "updated_at": "2018-07-25T01:54:14",
        "enterprise_project_id": "0aad99bc-f5f6-4f78-8404-c598d76b0ed2"
```



```
    }
}
```

Status Code

For details, see **Status Codes**.

6.1.2 Querying Load Balancers

Function

This API is used to query load balancers and display them in a list. Filter query and pagination query are supported.

Unless otherwise specified, exact match is applied.

URI

GET /v2/{project_id}/elb/loadbalancers

Table 6-9 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Table 6-10 Query parameters

Parameter	Mandatory	Type	Description
marker	No	String	Specifies the ID of the load balancer from which pagination query starts, that is, the ID of the last load balancer on the previous page. This parameter must be used together with **limit**.
limit	No	Integer	Specifies the number of load balancers on each page. If this parameter is not set, all load balancers are queried by default.

Parameter	Mandatory	Type	Description
page_reverse	No	Boolean	Specifies the page direction. The value can be **true** or **false**, and the default value is **false**. The last page in the list requested with **page_reverse** set to **false** will not contain the "next" link, and the last page in the list requested with **page_reverse** set to **true** will not contain the "previous" link. This parameter must be used together with **limit**.
id	No	String	Specifies the load balancer ID.
description	No	String	Provides supplementary information about the load balancer. The value contains a maximum of 255 characters.
name	No	String	Specifies the load balancer name. The value contains a maximum of 255 characters.
operating_status	No	String	Specifies the operating status of the load balancer. The value can be **ONLINE** or **FROZEN**.
provisioning_status	No	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the load balancer.
admin_state_up	No	Boolean	Specifies the administrative status of the load balancer. The load balancer stops receiving traffic after it is disabled. The value can be one of the following: **true**: Enable the load balancer. **false**: Disable the load balancer.
vip_address	No	String	Specifies the private IP address of the load balancer. The value contains a maximum of 64 characters.
vip_port_id	No	String	Specifies the ID of the port bound to the private IP address of the load balancer.
vip_subnet_id	No	String	Specifies the ID of the IPv4 subnet where the load balancer works.

Parameter	Mandatory	Type	Description
member_address	No	String	Specifies the IP address of the backend server associated with the load balancer.
member_device_id	No	String	Specifies the ID of the cloud server used as the backend server associated with the load balancer.
vpc_id	No	String	Specifies the ID of the VPC where the load balancer resides.
enterprise_project_id	No	String	Specifies the enterprise project ID. • If **enterprise_project_id** is not passed, resources in all enterprise projects are queried by default. Fine-grained authorization is performed. The **elb:*list** permissions must be assigned to the user group. • If **enterprise_project_id** is passed, the value can be a specific enterprise project ID or **all_granted_eps**. If the value is a specific enterprise project ID, only resources in the enterprise project are queried. If the value is **all_granted_eps**, resources in the enterprise projects with the **elb:*list** permissions are queried.

Request

None

Response

Table 6-11 Response parameters

Parameter	Type	Description
loadbalancers	Array of **Loadbalancers** objects	Lists the load balancers. For details, see **Table 6-12**.

Table 6-12 loadbalancer parameter description

Parameter	Type	Description
id	String	Specifies the load balancer ID.

Parameter	Type	Description
project_id	String	Specifies the ID of the project where the load balancer is used.
tenant_id	String	Specifies the tenant ID.
name	String	Specifies the load balancer name. The value contains a maximum of 255 characters.
description	String	Provides supplementary information about the load balancer. The value contains a maximum of 255 characters.
vip_subnet_id	String	Specifies the ID of the IPv4 subnet where the load balancer works.
vip_port_id	String	Specifies the ID of the port bound to the private IP address of the load balancer.
provider	String	Specifies the provider of the load balancer.
vip_address	String	Specifies the private IP address of the load balancer. The value contains a maximum of 64 characters.
listeners	Array of **Listeners** objects	Lists the IDs of listeners added to the load balancer. For details, see **Table 6-6**.
pools	Array of **Pools** objects	Lists the IDs of backend server groups associated with the load balancer. For details, see **Table 6-7**.
operating_status	String	Specifies the operating status of the load balancer. The value can be **ONLINE** or **FROZEN**.
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the load balancer.

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the load balancer. The load balancer stops receiving traffic after it is disabled. Value options: **true**: Enable a load balancer. **false**: Disable the load balancer.
tags	Array	Lists load balancer tags.
created_at	String	Specifies the time when the load balancer was created. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format. The value contains a maximum of 19 characters.
updated_at	String	Specifies the time when the load balancer was updated. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format. The value contains a maximum of 19 characters.
enterprise_project_id	String	Specifies the enterprise project ID. When creating a load balancer, you can assign an enterprise project to the load balancer. The value is character string **0** or a UUID with hyphens (-). Value **0** indicates the default enterprise project. **NOTE** For more information about enterprise projects and how to obtain enterprise project IDs, see **Enterprise Management User Guide**.

Parameter	Type	Description
charge_mode	String	Specifies how the load balancer will be billed. The value can be one of the following: • **flavor**: indicates the guaranteed performance that allows the load balancer to handle up to 50,000 concurrent connections, 5,000 connections and 5,000 queries per second. You will be charged if the load balancer provides guaranteed performance. • **null**: indicates that guaranteed performance is not provided.
billing_info	String	Specifies whether the billing information is left blank.
frozen_scene	String	Specifies the scenario where the load balancer is frozen. If there are multiple scenarios, separate them with commas (,). The value can be one of the following: • **POLICE**: The load balancer is frozen for public security. • **ILLEGAL**: The load balancer is frozen due to violation of laws and regulations. • **VERIFY**: The load balancer is frozen because the user fails to pass real-name authentication. • **PARTNER**: The load balancer is frozen by the partner. • **REAR**: Your account is in arrears.

Parameter	Type	Description
protection_status	String	Specifies whether modification protection is enabled. The value can be one of the following: • **nonProtection** (default): Modification protection is not enabled. • **consoleProtection**: Modification protection is enabled to avoid that resources are modified by accident on the console.
protection_reason	String	Specifies the reason to enable modification protection. This parameter is valid only when **protection_status** is set to **consoleProtection**.
publicips	Array of **PublicIpInfo** objects	Specifies the EIP bound to the load balancer. Only one EIP can be bound to a load balancer.

Table 6-13 listeners parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated listener.

Table 6-14 pools parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated backend server group.

Example Request

- Example request 1
  ```
  GET https://{Endpoint}/v2/1a3e005cf9ce40308c900bcb08e5320c/elb/loadbalancers
  ```
- Example request 2
  ```
  GET https://{Endpoint}/v2/1a3e005cf9ce40308c900bcb08e5320c/elb/loadbalancers?
  limit=10&marker=165b6a38-5278-4569-b747-b2ee65ea84a4
  ```
- Example request 3
  ```
  GET https://{Endpoint}/v2/601240b9c5c94059b63d484c92cfe308/elb/loadbalancers?
  member_address=192.168.0.198
  ```


Example Response

- Example response 1

```
{
   "loadbalancers": [
      {
         "description": "simple lb",
         "admin_state_up": true,
         "tenant_id": "1a3e005cf9ce40308c900bcb08e5320c",
         "project_id": "1a3e005cf9ce40308c900bcb08e5320c",
         "provisioning_status": "ACTIVE",
         "vip_subnet_id": "5328f1e6-ce29-44f1-9493-b128a5653350",
         "listeners": [
            {
               "id": "45196943-2907-4369-87b1-c009b1d7ac35"
            }
         ],
         "vip_address": "10.0.0.2",
         "vip_port_id": "cbced4fe-6f6f-4fd6-9348-0c3d1219d6ca",
         "provider": "vlb",
         "pools": [
            {
               "id": "21d49cf7-4fd3-4cb6-8c48-b7fc6c259aab"
             }
         ],
         "id": "a9729389-6147-41a3-ab22-a24aed8692b2",
         "operating_status": "ONLINE",
         "tags": [],
         "name": "loadbalancer1",
         "created_at": "2018-07-25T01:54:13",
         "updated_at": "2018-07-25T01:54:14",
         "enterprise_project_id": "0aad99bc-f5f6-4f78-8404-c598d76b0ed2"
      }
]
}
```

- Example response 2

```
{
   "loadbalancers": [
      {
         "description": "",
         "provisioning_status": "ACTIVE",
         "tenant_id": "601240b9c5c94059b63d484c92cfe308",
         "project_id": "601240b9c5c94059b63d484c92cfe308",
         "admin_state_up": true,
         "provider": "vlb",
         "pools": [
            {
               "id": "b13dba4c-a44c-4c40-8f6e-ce7a162b9f22"
            },
            {
               "id": "4b9e765f-82ee-4128-911b-0a2d9ebc74c7"
            }
         ],
         "listeners": [
            {
               "id": "21c41336-d0d3-4349-8641-6e82b4a4d097"
            }
         ],
         "vip_port_id": "44ac5d9b-b0c0-4810-9a9d-c4dbf541e47e",
         "operating_status": "ONLINE",
         "vip_address": "192.168.0.234",
         "vip_subnet_id": "9d60827e-0e5c-490a-8183-0b6ebf9084ca",
         "id": "e79a7dd6-3a38-429a-95f9-c7f78b346cbe",
         "tags": [],
         "name": "elb-robot",
         "created_at": "2018-07-25T01:54:13",
         "updated_at": "2018-07-25T01:54:14",
         "enterprise_project_id": "0aad99bc-f5f6-4f78-8404-c598d76b0ed2"
      }
```



```
    ]

}
```

- Example response 3

```
{
   "loadbalancers": [
      {
         "description": "",
         "provisioning_status": "ACTIVE",
         "tenant_id": "601240b9c5c94059b63d484c92cfe308",
         "project_id": "601240b9c5c94059b63d484c92cfe308",
         "admin_state_up": true,
         "provider": "vlb",
         "pools": [
            {
               "id": "ed75f16e-fcc6-403e-a3fb-4eae82005eab"
            },
            {
               "id": "f15f2723-4135-4bf8-9259-047d92684197"
            }
         ],
         "listeners": [
            {
               "id": "75045172-70e9-480d-9443-b8b6459948f7"
            },
            {
               "id": "b9a99cbb-d0a1-4269-bc5f-752ec37a10c3"
            }
         ],
         "vip_port_id": "fb3f10f0-9417-4cf2-a82e-8f1da1687484",
         "operating_status": "ONLINE",
         "vip_address": "192.168.0.16",
         "vip_subnet_id": "3a450aa4-f642-4da8-b70d-cafd4a633b51",
         "id": "bc7ba445-035a-4464-a1a3-a62cf4a14116",
         "tags": [],
         "name": "elb-hm-test",
         "created_at": "2018-07-25T01:54:13",
         "updated_at": "2018-07-25T01:54:14",
         "enterprise_project_id": "0aad99bc-f5f6-4f78-8404-c598d76b0ed2"
      }
   ]
}
```

Status Code

For details, see **Status Codes**.

6.1.3 Querying Details of a Load Balancer

Function

This API is used to query details about a load balancer using its ID.

URI

GET /v2/{project_id}/elb/loadbalancers/{loadbalancer_id}

Table 6-15 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
loadbalancer_id	Yes	String	Specifies the load balancer ID.

Request

None

Response

Table 6-16 Response parameters

Parameter	Type	Description
loadbalancer	**Loadbalancer** object	Specifies the load balancer. For details, see **Table 6-17**.

Table 6-17 loadbalancer parameter description

Parameter	Type	Description
id	String	Specifies the load balancer ID.
project_id	String	Specifies the ID of the project where the load balancer is used.
tenant_id	String	Specifies the tenant ID.
name	String	Specifies the load balancer name. The value contains a maximum of 255 characters.
description	String	Provides supplementary information about the load balancer. The value contains a maximum of 255 characters.
vip_subnet_id	String	Specifies the ID of the IPv4 subnet where the load balancer works.
vip_port_id	String	Specifies the ID of the port bound to the private IP address of the load balancer.

Parameter	Type	Description
provider	String	Specifies the provider of the load balancer.
vip_address	String	Specifies the private IP address of the load balancer. The value contains a maximum of 64 characters.
listeners	Array of **Listeners** objects	Lists the IDs of listeners added to the load balancer. For details, see **Table 6-6**.
pools	Array of **Pools** objects	Lists the IDs of backend server groups associated with the load balancer. For details, see **Table 6-7**.
operating_status	String	Specifies the operating status of the load balancer. The value can be **ONLINE** or **FROZEN**.
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the load balancer.
admin_state_up	Boolean	Specifies the administrative status of the load balancer. The load balancer stops receiving traffic after it is disabled. Value options: **true**: Enable a load balancer. **false**: Disable the load balancer.
tags	Array	Lists load balancer tags.
created_at	String	Specifies the time when the load balancer was created. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format. The value contains a maximum of 19 characters.
updated_at	String	Specifies the time when the load balancer was updated. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format. The value contains a maximum of 19 characters.

Parameter	Type	Description
enterprise_project_id	String	Specifies the enterprise project ID. When creating a load balancer, you can assign an enterprise project to the load balancer. The value is character string **0** or a UUID with hyphens (-). Value **0** indicates the default enterprise project. **NOTE** For more information about enterprise projects and how to obtain enterprise project IDs, see **Enterprise Management User Guide**.
charge_mode	String	Specifies how the load balancer will be billed. The value can be one of the following: • **flavor**: indicates the guaranteed performance that allows the load balancer to handle up to 50,000 concurrent connections, 5,000 connections and 5,000 queries per second. You will be charged if the load balancer provides guaranteed performance. • **null**: indicates that guaranteed performance is not provided.
billing_info	String	Specifies whether the billing information is left blank.

Parameter	Type	Description
frozen_scene	String	Specifies the scenario where the load balancer is frozen. If there are multiple scenarios, separate them with commas (,). The value can be one of the following: • **POLICE**: The load balancer is frozen for public security. • **ILLEGAL**: The load balancer is frozen due to violation of laws and regulations. • **VERIFY**: The load balancer is frozen because the user fails to pass real-name authentication. • **PARTNER**: The load balancer is frozen by the partner. • **REAR**: Your account is in arrears.
protection_status	String	Specifies whether modification protection is enabled. The value can be one of the following: • **nonProtection** (default): Modification protection is not enabled. • **consoleProtection**: Modification protection is enabled to avoid that resources are modified by accident on the console.
protection_reason	String	Specifies the reason to enable modification protection. This parameter is valid only when **protection_status** is set to **consoleProtection**.
publicips	Array of **PublicIpInfo** objects	Specifies the EIP bound to the load balancer. Only one EIP can be bound to a load balancer.

Table 6-18 listeners parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated listener.

Table 6-19 pools parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated backend server group.

Example Request

- Example request
  GET https://{Endpoint}/v2/1867112d054b427e808cc6096d8193a1/elb/loadbalancers/3d77894d-2ffe-4411-ac0a-0d57689779b8

Example Response

- Example response

```
{
    "loadbalancer": {
        "description": "",
        "admin_state_up": true,
        "tenant_id": "1867112d054b427e808cc6096d8193a1",
        "project_id": "1867112d054b427e808cc6096d8193a1",
        "provisioning_status": "ACTIVE",
        "vip_subnet_id": "4f5e8efe-fbbe-405e-b48c-a41202ef697c",
        "listeners": [
            {
                "id": "09e64049-2ab0-4763-a8c5-f4207875dc3e"
            }
        ],
        "vip_address": "192.168.2.4",
        "vip_port_id": "c7157e7a-036a-42ca-8474-100be22e3727",
        "provider": "vlb",
        "pools": [
            {
                "id": "b7e53dbd-62ab-4505-a280-5c066078a5c9"
            }
        ],
        "id": "3d77894d-2ffe-4411-ac0a-0d57689779b8",
        "operating_status": "ONLINE",
        "tags": [],
        "name": "lb-2",
        "created_at": "2018-07-25T01:54:13",
        "updated_at": "2018-07-25T01:54:14",
        "enterprise_project_id": "0aad99bc-f5f6-4f78-8404-c598d76b0ed2"
    }
}
```

Status Code

For details, see **Status Codes**.

6.1.4 Querying the Status Tree of a Load Balancer

Function

This API is used to query the status tree of a load balancer. You can use this API to query details about the associated listeners, backend server groups, backend servers, health checks, forwarding policies, and forwarding rules, helping you understand the topology of resources associated with the load balancer.

URI

GET /v2/{project_id}/elb/loadbalancers/{loadbalancer_id}/statuses

Table 6-20 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
loadbalancer_id	Yes	String	Specifies the load balancer ID.

Request

None

Response

Table 6-21 Parameter description

Parameter	Type	Description
statuses	**Statuses** object	Specifies the status tree of a load balancer. For details, see **Table 6-22**.

Table 6-22 statuses parameter description

Parameter	Type	Description
loadbalancer	**Loadbalancer** object	Specifies the load balancer. For details, see **Table 6-23**.

Table 6-23 loadbalancer parameter description

Parameter	Type	Description
id	String	Specifies the load balancer ID.
name	String	Specifies the load balancer name. The value contains a maximum of 255 characters.
listeners	Array of **Listeners** objects	Lists the listeners added to the load balancer. For details of this parameter, see **Table 6-24**.

Parameter	Type	Description
pools	Array of **Pools** objects	Lists the backend server groups associated with the load balancer. For details of this parameter, see **Table 6-25**.
operating_status	String	This field is reserved. It specifies the operating status of the load balancer. The value can be one of the following: • **ONLINE** (default): The load balancer is running normally. • **DEGRADED**: This status is displayed only when **provisioning_status** of a forwarding policy or forwarding rule added to a listener of the load balancer is set to **ERROR** and the API for querying the load balancer status tree is called. • **DISABLED**: This status is displayed only when **admin_state_up** of the load balancer is set to **false** and the API for querying the load balancer status tree is called. • **FROZEN**: The load balancer is frozen.
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the load balancer.

Table 6-24 listeners parameter description

Parameter	Type	Description
id	String	Specifies the listener ID.
name	String	Specifies the listener name.
l7policies	Array of **l7policies** objects	Lists associated forwarding policies. For details of this parameter, see **Table 6-28**.

Parameter	Type	Description
pools	Array of **Pools** objects	Lists the backend server groups associated with the listener. For details of this parameter, see **Table 6-25**.
operating_status	String	This parameter is reserved, and its value can only be **ONLINE**. It specifies the operating status of the listener.
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the listener.

Table 6-25 pools parameter description

Parameter	Type	Description
id	String	Specifies the ID of the backend server group.
name	String	Specifies the name of the backend server group.
healthmonitor	**Healthmonitor** object	Provides health check details of the backend server group. For details of this parameter, see **Table 6-26**.
members	Array of **Members** objects	Lists the members contained in the backend server group. For details of this parameter, see **Table 6-27**.
operating_status	String	This parameter is reserved, and its value can only be **ONLINE**. It specifies the operating status of the backend server group.
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the backend server group.

Table 6-26 healthmonitor parameter description

Parameter	Type	Description
id	String	Specifies the health check ID.
name	String	Specifies the health check name.
type	String	• Specifies the health check protocol. • The value can be **UDP_CONNECT**, **TCP**, or **HTTP**.
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the health check.

Table 6-27 members parameter description

Parameter	Type	Description
id	String	Specifies the backend server ID.
address	String	Specifies the private IP address of the backend server, for example, 192.168.3.11.
protocol_port	Integer	• Specifies the port used by the backend server. • The port number ranges from 0 to 65535.

Parameter	Type	Description
operating_status	String	This parameter is reserved. It specifies the operating status of the backend server. The value can be one of the following: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group that the backend server belongs to. • **DISABLED**: The backend server is not available. This status is displayed only when **admin_state_up** of the backend server, or the backend server group to which it belongs, or the associated load balancer is set to **false** and the API for querying the load balancer status tree is called. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist. **NOTE** When **admin_state_up** is set to **false** and **operating_status** is set to **OFFLINE** for a backend server, **DISABLED** is returned for **operating_status** of the backend server in the response of this API.
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the backend server.

Table 6-28 l7policies parameter description

Parameter	Type	Description
id	String	Specifies the forwarding policy ID.
name	String	Specifies the forwarding policy name.

Parameter	Type	Description
rules	Array of **Rules** objects	Lists the forwarding rules of the forwarding policy. For details of this parameter, see **Table 6-29**.
action	String	• Specifies whether requests are forwarded to another backend server group or redirected to an HTTPS listener. • The value can be **REDIRECT_TO_POOL** or **REDIRECT_TO_LISTENER**. REDIRECT_TO_POOL: Requests are forwarded to another backend server group. **REDIRECT_TO_LISTENER**: Requests are redirected to an HTTPS listener.
provisioning_status	String	This parameter is reserved. It specifies the provisioning status of the forwarding policy. The value can be one of the following: • **ACTIVE** (default): The forwarding policy is normal. • **ERROR**: Another forwarding policy of the same listener has the same forwarding rule.

Table 6-29 rules parameter description

Parameter	Type	Description
id	String	Specifies the forwarding rule ID.
type	String	• Specifies the match type of a forwarding rule. • The value can be **PATH** or **HOST_NAME**. PATH: matches the path in the request. **HOST_NAME**: matches the domain name in the request.

Parameter	Type	Description
provisioning_status	String	This parameter is reserved. It specifies the provisioning status of the forwarding rule. The value can be one of the following: • **ACTIVE** (default): The forwarding rule is normal. • **ERROR**: Another forwarding policy of the same listener has the same forwarding rule.

Example Request

- Example request
  GET https://{Endpoint}/v2/145483a5107745e9b3d80f956713e6a3/elb/loadbalancers/38278031-cfca-44be-81be-a412f618773b/statuses

Example Response

- Example response

```
{
   "statuses": {
      "loadbalancer": {
         "name": "lb-jy",
         "provisioning_status": "ACTIVE",
         "listeners": [
            {
               "name": "listener-jy-1",
               "provisioning_status": "ACTIVE",
               "pools": [
                  {
                     "name": "pool-jy-1",
                     "provisioning_status": "ACTIVE",
                     "healthmonitor": {
                        "type": "TCP",
                        "id": "7422b51a-0ed2-4702-9429-4f88349276c6",
                        "name": "",
                        "provisioning_status": "ACTIVE"
                     },
                     "members": [
                        {
                           "protocol_port": 80,
                           "address": "192.168.44.11",
                           "id": "7bbf7151-0dce-4087-b316-06c7fa17b894",
                           "operating_status": "ONLINE",
                           "provisioning_status": "ACTIVE"
                        }
                     ],
                     "id": "c54b3286-2349-4c5c-ade1-e6bb0b26ad18",
                     "operating_status": "ONLINE"
                  }
               ],
               "l7policies": [],
               "id": "eb84c5b4-9bc5-4bee-939d-3900fb05dc7b",
               "operating_status": "ONLINE"
            }
         ],
```



```
        "pools": [
          {
            "name": "pool-jy-1",
            "provisioning_status": "ACTIVE",
            "healthmonitor": {
              "type": "TCP",
              "id": "7422b51a-0ed2-4702-9429-4f88349276c6",
              "name": "",
              "provisioning_status": "ACTIVE"
            },
            "members": [
              {
                "protocol_port": 80,
                "address": "192.168.44.11",
                "id": "7bbf7151-0dce-4087-b316-06c7fa17b894",
                "operating_status": "ONLINE",
                "provisioning_status": "ACTIVE"
              }
            ],
            "id": "c54b3286-2349-4c5c-ade1-e6bb0b26ad18",
            "operating_status": "ONLINE"
          }
        ],
        "id": "38278031-cfca-44be-81be-a412f618773b",
        "operating_status": "ONLINE"
      }
    }
}
```


Status Code

For details, see **Status Codes**.

6.1.5 Updating a Load Balancer

Function

This API is used to update the name or description of a load balancer.

URI

PUT /v2/{project_id}/elb/loadbalancers/{loadbalancer_id}

Table 6-30 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
loadbalancer_id	Yes	String	Specifies the load balancer ID.

Request

Table 6-31 Parameter description

Parameter	Mandatory	Type	Description
loadbalancer	Yes	**Loadbalancer** object	Specifies the load balancer. For details, see **Table 6-32**.

Table 6-32 loadbalancer parameter description

Parameter	Mandatory	Type	Description
name	No	String	Specifies the load balancer name. The value contains a maximum of 255 characters.
description	No	String	Provides supplementary information about the load balancer. The value contains a maximum of 255 characters.
admin_state_up	No	Boolean	Specifies the administrative status of the load balancer. The load balancer stops receiving traffic after it is disabled. The value can be one of the following: **true**: Enable the load balancer. **false**: Disable the load balancer.

Parameter	Mandatory	Type	Description
protection_status	No	String	Specifies whether modification protection is enabled. The value can be one of the following: • **nonProtection** (default): Modification protection is not enabled. • **consoleProtection**: Modification protection is enabled to avoid that resources are modified by accident on the console.
protection_reason	No	String	Specifies the reason to enable modification protection. This parameter is valid only when **protection_status** is set to **consoleProtection**.

Response

Table 6-33 Response parameters

Parameter	Type	Description
loadbalancer	**Loadbalancer** object	Specifies the load balancer. For details, see **Table 6-34**.

Table 6-34 loadbalancer parameter description

Parameter	Type	Description
id	String	Specifies the load balancer ID.
project_id	String	Specifies the ID of the project where the load balancer is used.
tenant_id	String	Specifies the tenant ID.

Parameter	Type	Description
name	String	Specifies the load balancer name. The value contains a maximum of 255 characters.
description	String	Provides supplementary information about the load balancer. The value contains a maximum of 255 characters.
vip_subnet_id	String	Specifies the ID of the IPv4 subnet where the load balancer works.
vip_port_id	String	Specifies the ID of the port bound to the private IP address of the load balancer.
provider	String	Specifies the provider of the load balancer.
vip_address	String	Specifies the private IP address of the load balancer. The value contains a maximum of 64 characters.
listeners	Array of **Listeners** objects	Lists the IDs of listeners added to the load balancer. For details, see **Table 6-6**.
pools	Array of **Pools** objects	Lists the IDs of backend server groups associated with the load balancer. For details, see **Table 6-7**.
operating_status	String	Specifies the operating status of the load balancer. The value can be **ONLINE** or **FROZEN**.
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the load balancer.

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the load balancer. The load balancer stops receiving traffic after it is disabled. Value options: **true**: Enable a load balancer. **false**: Disable the load balancer.
tags	Array	Lists load balancer tags.
created_at	String	Specifies the time when the load balancer was created. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format. The value contains a maximum of 19 characters.
updated_at	String	Specifies the time when the load balancer was updated. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format. The value contains a maximum of 19 characters.
enterprise_project_id	String	Specifies the enterprise project ID. When creating a load balancer, you can assign an enterprise project to the load balancer. The value is character string **0** or a UUID with hyphens (-). Value **0** indicates the default enterprise project. **NOTE** For more information about enterprise projects and how to obtain enterprise project IDs, see **Enterprise Management User Guide**.

Parameter	Type	Description
charge_mode	String	Specifies how the load balancer will be billed. The value can be one of the following: • **flavor**: indicates the guaranteed performance that allows the load balancer to handle up to 50,000 concurrent connections, 5,000 connections and 5,000 queries per second. You will be charged if the load balancer provides guaranteed performance. • **null**: indicates that guaranteed performance is not provided.
billing_info	String	Specifies whether the billing information is left blank.
frozen_scene	String	Specifies the scenario where the load balancer is frozen. If there are multiple scenarios, separate them with commas (,). The value can be one of the following: • **POLICE**: The load balancer is frozen for public security. • **ILLEGAL**: The load balancer is frozen due to violation of laws and regulations. • **VERIFY**: The load balancer is frozen because the user fails to pass real-name authentication. • **PARTNER**: The load balancer is frozen by the partner. • **REAR**: Your account is in arrears.

Parameter	Type	Description
protection_status	String	Specifies whether modification protection is enabled. The value can be one of the following: • **nonProtection** (default): Modification protection is not enabled. • **consoleProtection**: Modification protection is enabled to avoid that resources are modified by accident on the console.
protection_reason	String	Specifies the reason to enable modification protection. This parameter is valid only when **protection_status** is set to **consoleProtection**.
publicips	Array of **PublicIpInfo** objects	Specifies the EIP bound to the load balancer. Only one EIP can be bound to a load balancer.

Table 6-35 listeners parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated listener.

Table 6-36 pools parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated backend server group.

Example Request

- Example request

```
PUT https://{Endpoint}/v2/145483a5107745e9b3d80f956713e6a3/elb/loadbalancers/
1e11b74e-30b7-4b78-b09b-84aec4a04487

{
   "loadbalancer": {
      "name": "lb_update_test",
      "description": "lb update test"
   }
}
```


Example Response

- Example response

```
{
  "loadbalancer": {
    "description": "simple lb2",
    "admin_state_up": true,
    "tenant_id": "145483a5107745e9b3d80f956713e6a3",
    "project_id": "145483a5107745e9b3d80f956713e6a3",
    "provisioning_status": "ACTIVE",
    "vip_subnet_id": "823d5866-6e30-45c2-9b1a-a1ebc3757fdb",
    "listeners": [
      {
        "id": "37ffe679-08ef-436e-b6bd-cf66fb4c3de2"
      }
    ],
    "vip_address": "192.172.1.68",
    "vip_port_id": "f42e3019-67f7-4d2a-8d1c-af49e7c22fa6",
    "provider": "vlb",
    "tags": [],
    "pools": [
      {
        "id": "75c4f2d4-a213-4408-9fa8-d64708e8d1df"
      }
    ],
    "id": "c32a9f9a-0cc6-4f38-bb9c-cde79a533c19",
    "operating_status": "ONLINE",
    "name": "loadbalancer-test2",
    "created_at": "2018-07-25T01:54:13",
    "updated_at": "2018-07-25T01:54:14",
    "enterprise_project_id": "0aad99bc-f5f6-4f78-8404-c598d76b0ed2"
  }
}
```

Status Code

For details, see **Status Codes**.

6.1.6 Deleting a Load Balancer

Function

This API is used to delete a load balancer by ID.

Constraints

When you set **cascade** to **false**, you must delete the resources associated with the load balancer before attempting to delete it.

URI

DELETE /v2/{project_id}/elb/loadbalancers/{loadbalancer_id}

Table 6-37 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Parameter	Mandatory	Type	Description
loadbalancer_id	Yes	String	Specifies the load balancer ID.
cascade	No	Boolean	Specifies whether to delete the resources associated with the load balancer when it is deleted, including the listeners, backend server groups, and backend servers.

Request

None

Response

None

Example Request

- Example request
  DELETE https://{Endpoint}/v2/145483a5107745e9b3d80f956713e6a3/elb/loadbalancers/90f7c765-0bc9-47c4-8513-4cc0c264c8f8

Example Response

- Example response
  None

Status Code

For details, see **Status Codes**.

6.2 Listener

6.2.1 Adding a Listener

Function

This API is used to add a listener to a load balancer.

Constraints

- Only users with the ELB administrator permissions can specify the value of **connection_limit**.
- The value of **protocol** can be **TCP**, **HTTP**, **UDP**, or **TERMINATED_HTTPS**.

URI

POST /v2/{project_id}/elb/listeners

Table 6-38 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Request

Table 6-39 Parameter description

Parameter	Mandatory	Type	Description
listener	Yes	**Listener** object	Specifies the listener. For details, see **Table 6-40**.

Table 6-40 listener parameter description

Parameter	Mandatory	Type	Description
tenant_id	No	String	Specifies the ID of the project where the listener is used. The value must be the same as the value of **project_id** in the token. The value contains a maximum of 255 characters.
name	No	String	Specifies the listener name. Note: If you leave the listener name empty, you cannot locate it on the listener list and view its details. The value contains a maximum of 255 characters.
description	No	String	Provides supplementary information about the listener. The value contains a maximum of 255 characters.

Parameter	Mandatory	Type	Description
protocol	Yes	String	Specifies the protocol used by the listener. The value can be **TCP**, **HTTP**, **UDP**, or **TERMINATED_HTTPS**.
protocol_port	Yes	Integer	Specifies the port used by the listener. The port number ranges from 1 to 65535. **NOTE** • If the protocol used by the listener is UDP, the port number cannot be 4789. • HTTP and TERMINATED_HTTPS listeners cannot use port 21.
loadbalancer_id	Yes	String	Specifies the ID of the associated load balancer.
connection_limit	No	Integer	Specifies the maximum number of connections. The value ranges from **-1** to **2147483647**. The default value is **-1**, indicating that there is no restriction on the maximum number of connections. This parameter is reserved.
admin_state_up	No	Boolean	Specifies the administrative status of the listener. This parameter is reserved, and the default value is **true**.
http2_enable	No	Boolean	Specifies whether to use HTTP/2. The value can be **true** or **false**. • **true**: HTTP/2 will be used. • **false**: HTTP/2 will not be used. The default value is **false**. This parameter takes effect only when the protocol used by the listener is set to **TERMINATED_HTTPS**.

Parameter	Mandatory	Type	Description
default_pool_id	No	String	Specifies the ID of the associated backend server group. If a request does not match the forwarding policy, the request is forwarded to the default backend server group for processing. If the value is **null**, the listener has no default backend server group. The **default_pool_id** parameter has the following constraints: ● Its value cannot be the ID of any backend server group of other listeners. ● Its value cannot be the ID of any backend server group associated with the forwarding policies set for other listeners. The relationships between the protocol of the backend server group and the protocol used by the listener are as follows: ● When the protocol used by the listener is **TCP**, the protocol of the backend server group must be **TCP**. ● When the protocol used by the listener is **UDP**, the protocol of the backend server group must be **UDP**. ● When the protocol used by the listener is **HTTP** or **TERMINATED_HTTPS**, the protocol of the backend server group must be **HTTP**.

Parameter	Mandatory	Type	Description
default_tls_container_ref	No	String	Specifies the ID of the server certificate used by the listener. This parameter is mandatory when **protocol** is set to **TERMINATED_HTTPS**. The default value is **null** when **protocol** is not set to **TERMINATED_HTTPS**. The value contains a maximum of 128 characters. **NOTE** This parameter takes effect only when the protocol used by the listener is set to **TERMINATED_HTTPS**.
client_ca_tls_container_ref	No	String	Specifies the ID of the CA certificate used by the listener. The default value is **null**. The value contains a maximum of 128 characters. **NOTE** This parameter takes effect only when the protocol used by the listener is set to **TERMINATED_HTTPS**.
sni_container_refs	No	Array	Lists the IDs of SNI certificates (server certificates with domain names) used by the listener. If the parameter value is an empty list, the SNI feature is disabled. The default value is **[]**. **NOTE** This parameter takes effect only when the protocol used by the listener is set to **TERMINATED_HTTPS**.

Parameter	Mandatory	Type	Description
insert_headers	No	InsertHeaders object	Specifies whether to insert HTTP extension headers and sent them to backend servers. All headers are synchronized. If this parameter is not set, default values are used. Information required by backend servers can be written into HTTP headers and passed to backend servers. For example, you can use the **X-Forwarded-ELB-IP** header to transmit the load balancer EIP to backend servers. For details, see Table 6-41. **NOTE** This parameter takes effect only when the protocol used by the listener is set to **HTTP** or **TERMINATED_HTTPS**.
tls_ciphers_policy	No	String	Specifies the security policy used by the listener. This parameter takes effect only when the protocol used by the listener is set to **TERMINATED_HTTPS**. The value can be **tls-1-0-inherit**, **tls-1-0**, **tls-1-1**, **tls-1-2**, or **tls-1-2-strict**, and the default value is **tls-1-0**. For details of cipher suites for each security policy, see Table 6-42.
protection_status	No	String	Specifies whether modification protection is enabled. The value can be one of the following: • **nonProtection** (default): Modification protection is not enabled. • **consoleProtection**: Modification protection is enabled to avoid that resources are modified by accident on the console.
protection_reason	No	String	Specifies the reason to enable modification protection. This parameter is valid only when **protection_status** is set to **consoleProtection**.

Table 6-41 insert_headers parameter description

Parameter	Mandatory	Type	Description
X-Forwarded-ELB-IP	No	Boolean	Specifies whether to transparently transmit the load balancer EIP to backend servers. After this function is enabled, the load balancer EIP is stored in the HTTP header and passes to backend servers. The value can be **true** or **false**. **true**: This function is enabled. **false**: The function is disabled. The function is disabled by default.
X-Forwarded-Host	No	Boolean	Specifies whether to rewrite the **X-Forwarded-Host** header. If this function is enabled, **X-Forwarded-Host** is rewritten based on **Host** in the request and sent to backend servers. The value can be **true** or **false**. **true**: This function is enabled. **false**: The function is disabled. The function is enabled by default.

Table 6-42 tls_ciphers_policy parameter description

Security Policy	TLS Version	Cipher Suite
tls-1-0-inherit	TLS 1.2 TLS 1.1 TLS 1.0	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:DHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:AES128-SHA:AES256-SHA:DHE-DSS-AES128-SHA:CAMELLIA128-SHA:EDH-RSA-DES-CBC3-SHA:DES-CBC3-SHA:ECDHE-RSA-RC4-SHA:RC4-SHA:DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:DHE-RSA-CAMELLIA256-SHA:DHE-DSS-CAMELLIA256-SHA:CAMELLIA256-SHA:EDH-DSS-DES-CBC3-SHA:DHE-RSA-CAMELLIA128-SHA:DHE-DSS-CAMELLIA128-SHA

Security Policy	TLS Version	Cipher Suite
tls-1-0	TLS 1.2 TLS 1.1 TLS 1.0	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:AES128-SHA:AES256-SHA
tls-1-1	TLS 1.2 TLS 1.1	
tls-1-2	TLS 1.2	
tls-1-2-strict	TLS 1.2	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384

Response

Table 6-43 Response parameters

Parameter	Type	Description
listener	**Listener** object	Specifies the listener. For details, see **Table 6-44**.

Table 6-44 listener parameter description

Parameter	Type	Description
id	String	Specifies the listener ID.
tenant_id	String	Specifies the ID of the project where the listener is used. The value contains a maximum of 255 characters.
project_id	String	Specifies the ID of the project to which the listener belongs. This parameter has the same meaning as **tenant_id**.

Parameter	Type	Description
name	String	Specifies the listener name. Note: If you leave the listener name empty, you cannot locate it on the listener list and view its details. The value contains a maximum of 255 characters.
description	String	Provides supplementary information about the listener. The value contains a maximum of 255 characters.
protocol	String	Specifies the protocol used by the listener. The value can be **TCP**, **HTTP**, **UDP**, or **TERMINATED_HTTPS**.
protocol_port	Integer	Specifies the port used by the listener. The port number ranges from 1 to 65535.
loadbalancers	Array of **Loadbalancers** objects	Specifies the ID of the associated load balancer. For details, see **Table 6-45**.
connection_limit	Integer	Specifies the maximum number of connections. The value ranges from **-1** to **2147483647**. The default value is **-1**, indicating that there is no restriction on the maximum number of connections. This parameter is reserved.
admin_state_up	Boolean	Specifies the administrative status of the listener. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
http2_enable	Boolean	Specifies whether to use HTTP/2. The value can be **true** or **false**. • **true**: HTTP/2 is used. • **false**: HTTP/2 is not used. This parameter takes effect only when the protocol used by the listener is set to **TERMINATED_HTTPS**.

Parameter	Type	Description
default_pool_id	String	Specifies the ID of the associated backend server group. If a request does not match the forwarding policy, the request is forwarded to the default backend server group for processing. If the value is **null**, the listener has no default backend server group.
default_tls_container_ref	String	Specifies the ID of the server certificate used by the listener. For details, see **Certificate**. This parameter is mandatory when **protocol** is set to **TERMINATED_HTTPS**. The value contains a maximum of 128 characters.
client_ca_tls_container_ref	String	Specifies the ID of the CA certificate used by the listener. The value contains a maximum of 128 characters. For details, see **Certificate**.
sni_container_refs	Array	Lists the IDs of SNI certificates (server certificates with domain names) used by the listener. If the parameter value is an empty list, the SNI feature is disabled.
tags	Array	Tags the listener.
created_at	String	Specifies the time when the listener was created. YYYY-MM-DDTHH:MM:SS
updated_at	String	Specifies the time when the listener was updated. YYYY-MM-DDTHH:MM:SS
insert_headers	**InsertHeaders** object	Specifies whether to insert HTTP extension headers and sent them to backend servers. All headers are synchronized. If this parameter is not set, default values are used. Information required by backend servers can be written into HTTP headers and passed to backend servers. For example, you can use the **X-Forwarded-ELB-IP** header to transmit the load balancer EIP to backend servers. For details, see **Table 6-46**.

Parameter	Type	Description
tls_ciphers_policy	String	Specifies the security policy used by the listener. This parameter takes effect only when the protocol used by the listener is set to **TERMINATED_HTTPS**. The value can be **tls-1-0-inherit**, **tls-1-0**, **tls-1-1**, **tls-1-2**, or **tls-1-2-strict**, and the default value is **tls-1-0**. Lists cipher suites used by each security policy. For details, see **Table 6-47**.
protection_status	String	String Specifies whether modification protection is enabled. The value can be one of the following: • **nonProtection** (default): Modification protection is not enabled. • **consoleProtection**: Modification protection is enabled to avoid that resources are modified by accident on the console.
protection_reason	String	String Specifies the reason to enable modification protection. This parameter is valid only when **protection_status** is set to **consoleProtection**.

Table 6-45 loadbalancers parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	Specifies the ID of the associated load balancer.

Table 6-46 insert_headers parameter description

Parameter	Mandatory	Type	Description
X-Forwarded-ELB-IP	No	Boolean	Specifies whether to transparently transmit the load balancer EIP to backend servers. After this function is enabled, the load balancer EIP is stored in the HTTP header and passes to backend servers. The value can be **true** or **false**. **true**: This function is enabled. **false**: The function is disabled. The function is disabled by default.
X-Forwarded-Host	No	Boolean	Specifies whether to rewrite the **X-Forwarded-Host** header. If this function is enabled, **X-Forwarded-Host** is rewritten based on **Host** in the request and sent to backend servers. The value can be **true** or **false**. **true**: This function is enabled. **false**: The function is disabled. The function is enabled by default.

Table 6-47 tls_ciphers_policy parameter description

Security Policy	TLS Version	Cipher Suite
tls-1-0-inherit	TLS 1.2 TLS 1.1 TLS 1.0	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:DHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:AES128-SHA:AES256-SHA:DHE-DSS-AES128-SHA:CAMELLIA128-SHA:EDH-RSA-DES-CBC3-SHA:DES-CBC3-SHA:ECDHE-RSA-RC4-SHA:RC4-SHA:DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:DHE-RSA-CAMELLIA256-SHA:DHE-DSS-CAMELLIA256-SHA:CAMELLIA256-SHA:EDH-DSS-DES-CBC3-SHA:DHE-RSA-CAMELLIA128-SHA:DHE-DSS-CAMELLIA128-SHA

Security Policy	TLS Version	Cipher Suite
tls-1-0	TLS 1.2 TLS 1.1 TLS 1.0	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:AES128-SHA:AES256-SHA
tls-1-1	TLS 1.2 TLS 1.1	
tls-1-2	TLS 1.2	
tls-1-2-strict	TLS 1.2	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384

Example Request

- Example request 1: Adding a TCP listener

```
POST https://{Endpoint}/v2/145483a5107745e9b3d80f956713e6a3/elb/listeners

{
    "listener": {
        "protocol_port": 80,
        "protocol": "TCP",
        "loadbalancer_id": "0416b6f1-877f-4a51-987e-978b3f084253",
        "name": "listener-test",
        "insert_headers":{},

        "admin_state_up": true
    }
}
```

- Example request 2: Adding a listener with **protocol** set to **TERMINATED_HTTPS**

```
POST https://{Endpoint}/v2/601240b9c5c94059b63d484c92cfe308/elb/listeners

{
    "listener": {
        "protocol_port": 25,
        "protocol": "TERMINATED_HTTPS",
        "default_tls_container_ref": "02dcd56799e045bf8b131533cc911dd6",
        "loadbalancer_id": "0416b6f1-877f-4a51-987e-978b3f084253",
        "name": "listener-test",
        "admin_state_up": true
    }
}
```


Example Response

- Example response 1

```
{
   "listener": {
      "protocol_port": 80,
      "protocol": "TCP",
      "description": "",
      "client_ca_tls_container_ref": null,
      "default_tls_container_ref": null,
      "admin_state_up": true,
      "http2_enable": false,
      "loadbalancers": [
         {
            "id": "0416b6f1-877f-4a51-987e-978b3f084253"
         }
      ],
      "tenant_id": "145483a5107745e9b3d80f956713e6a3",
      "project_id": "145483a5107745e9b3d80f956713e6a3",
      "sni_container_refs": [],
      "connection_limit": -1,
      "default_pool_id": null,
      "tags": [],
      "insert_headers":{},
      "id": "b7f32b52-6f17-4b16-9ec8-063d71b653ce",
      "name": "listener-test",
      "created_at": "2018-07-25T01:54:13",
      "updated_at": "2018-07-25T01:54:14"
    }
}
```

- Example response 2

```
{
   "listener": {
      "insert_headers": {},
      "protocol_port": 25,
      "protocol": "TERMINATED_HTTPS",
      "description": "",
      "default_tls_container_ref": "02dcd56799e045bf8b131533cc911dd6",
      "sni_container_refs": [],
      "loadbalancers": [
         {
            "id": "0416b6f1-877f-4a51-987e-978b3f084253"
         }
      ],
      "tenant_id": "601240b9c5c94059b63d484c92cfe308",
      "project_id": "601240b9c5c94059b63d484c92cfe308",
      "created_at": "2019-01-21T12:38:31",
      "client_ca_tls_container_ref": null,
      "connection_limit": -1,
      "updated_at": "2019-01-21T12:38:31",
      "http2_enable": false,
      "admin_state_up": true,
      "default_pool_id": null,
      "insert_headers":{},
      "id": "b56634cd-5ba8-460e-b5a2-6de5ba8eaf60",
      "tags": [],
      "name": "listener-test"
   }
}
```

- Example response 3

```
{
   "listener": {
      "insert_headers": {},
      "protocol_port": 27,
      "protocol": "TERMINATED_HTTPS",
      "description": "",
      "default_tls_container_ref": "02dcd56799e045bf8b131533cc911dd6",
      "sni_container_refs": [
```



```
            "5882325fd6dd4b95a88d33238d293a0f",
            "e15d1b5000474adca383c3cd9ddc06d4"
        ],
        "loadbalancers": [
            {
                "id": "6bb85e33-4953-457a-85a9-336d76125b7b"
            }
        ],
        "tenant_id": "601240b9c5c94059b63d484c92cfe308",
        "project_id": "601240b9c5c94059b63d484c92cfe308",
        "created_at": "2019-01-21T12:43:55",
        "client_ca_tls_container_ref": null,
        "connection_limit": -1,
        "updated_at": "2019-01-21T12:43:55",
        "http2_enable": false,
        "admin_state_up": true,
        "default_pool_id": null,
        "insert_headers":{},
        "id": "b2cfda5b-52fe-4320-8845-34e8d4dac2c7",
        "tags": [],
        "name": "listener-test"
    }
}
```


Status Code

For details, see **Status Codes**.

6.2.2 Querying Details of a Listener

Function

This API is used to query details about a listener using its ID.

URI

GET /v2/{project_id}/elb/listeners/{listener_id}

Table 6-48 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
listener_id	Yes	String	Specifies the listener ID.

Request

None

Response

Table 6-49 Response parameters

Parameter	Type	Description
listener	**Listener** object	Specifies the listener. For details, see **Table 6-50**.

Table 6-50 listener parameter description

Parameter	Type	Description
id	String	Specifies the listener ID.
tenant_id	String	Specifies the ID of the project where the listener is used. The value contains a maximum of 255 characters.
project_id	String	Specifies the ID of the project to which the listener belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the listener name. Note: If you leave the listener name empty, you cannot locate it on the listener list and view its details. The value contains a maximum of 255 characters.
description	String	Provides supplementary information about the listener. The value contains a maximum of 255 characters.
protocol	String	Specifies the protocol used by the listener. The value can be **TCP**, **HTTP**, **UDP**, or **TERMINATED_HTTPS**.
protocol_port	Integer	Specifies the port used by the listener. The port number ranges from 1 to 65535.
loadbalancers	Array of **Loadbalancers** objects	Specifies the ID of the associated load balancer. For details, see **Table 6-45**.

Parameter	Type	Description
connection_limit	Integer	Specifies the maximum number of connections. The value ranges from **-1** to **2147483647**. The default value is **-1**, indicating that there is no restriction on the maximum number of connections. This parameter is reserved.
admin_state_up	Boolean	Specifies the administrative status of the listener. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
http2_enable	Boolean	Specifies whether to use HTTP/2. The value can be **true** or **false**. • **true**: HTTP/2 is used. • **false**: HTTP/2 is not used. This parameter takes effect only when the protocol used by the listener is set to **TERMINATED_HTTPS**.
default_pool_id	String	Specifies the ID of the associated backend server group. If a request does not match the forwarding policy, the request is forwarded to the default backend server group for processing. If the value is **null**, the listener has no default backend server group.
default_tls_container_ref	String	Specifies the ID of the server certificate used by the listener. For details, see **Certificate**. This parameter is mandatory when **protocol** is set to **TERMINATED_HTTPS**. The value contains a maximum of 128 characters.
client_ca_tls_container_ref	String	Specifies the ID of the CA certificate used by the listener. The value contains a maximum of 128 characters. For details, see **Certificate**.

Parameter	Type	Description
sni_container_refs	Array	Lists the IDs of SNI certificates (server certificates with domain names) used by the listener. If the parameter value is an empty list, the SNI feature is disabled.
tags	Array	Tags the listener.
created_at	String	Specifies the time when the listener was created. YYYY-MM-DDTHH:MM:SS
updated_at	String	Specifies the time when the listener was updated. YYYY-MM-DDTHH:MM:SS
insert_headers	**InsertHeaders** object	Specifies whether to insert HTTP extension headers and sent them to backend servers. All headers are synchronized. If this parameter is not set, default values are used. Information required by backend servers can be written into HTTP headers and passed to backend servers. For example, you can use the **X-Forwarded-ELB-IP** header to transmit the load balancer EIP to backend servers. For details, see **Table 6-46**.
tls_ciphers_policy	String	Specifies the security policy used by the listener. This parameter takes effect only when the protocol used by the listener is set to **TERMINATED_HTTPS**. The value can be **tls-1-0-inherit**, **tls-1-0**, **tls-1-1**, **tls-1-2**, or **tls-1-2-strict**, and the default value is **tls-1-0**. Lists cipher suites used by each security policy. For details, see **Table 6-47**.
protection_status	String	String Specifies whether modification protection is enabled. The value can be one of the following: • **nonProtection** (default): Modification protection is not enabled. • **consoleProtection**: Modification protection is enabled to avoid that resources are modified by accident on the console.
protection_reason	String	String Specifies the reason to enable modification protection. This parameter is valid only when **protection_status** is set to **consoleProtection**.

Table 6-51 loadbalancers parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	Specifies the ID of the associated load balancer.

Table 6-52 insert_headers parameter description

Parameter	Mandatory	Type	Description
X-Forwarded-ELB-IP	No	Boolean	Specifies whether to transparently transmit the load balancer EIP to backend servers. After this function is enabled, the load balancer EIP is stored in the HTTP header and passes to backend servers. The value can be **true** or **false**. **true**: This function is enabled. **false**: The function is disabled. The function is disabled by default.
X-Forwarded-Host	No	Boolean	Specifies whether to rewrite the **X-Forwarded-Host** header. If this function is enabled, **X-Forwarded-Host** is rewritten based on **Host** in the request and sent to backend servers. The value can be **true** or **false**. **true**: This function is enabled. **false**: The function is disabled. The function is enabled by default.

Table 6-53 tls_ciphers_policy parameter description

Security Policy	TLS Version	Cipher Suite
tls-1-0-inherit	TLS 1.2 TLS 1.1 TLS 1.0	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:DHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:AES128-SHA:AES256-SHA:DHE-DSS-AES128-SHA:CAMELLIA128-SHA:EDH-RSA-DES-CBC3-SHA:DES-CBC3-SHA:ECDHE-RSA-RC4-SHA:RC4-SHA:DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:DHE-RSA-CAMELLIA256-SHA:DHE-DSS-CAMELLIA256-SHA:CAMELLIA256-SHA:EDH-DSS-DES-CBC3-SHA:DHE-RSA-CAMELLIA128-SHA:DHE-DSS-CAMELLIA128-SHA
tls-1-0	TLS 1.2 TLS 1.1 TLS 1.0	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:AES128-SHA:AES256-SHA
tls-1-1	TLS 1.2 TLS 1.1	
tls-1-2	TLS 1.2	
tls-1-2-strict	TLS 1.2	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384

Example Request

- Example request
  GET https://{Endpoint}/v2/1867112d054b427e808cc6096d8193a1/elb/listeners/09e64049-2ab0-4763-a8c5-f4207875dc3e

Example Response

- Example response

```
{
    "listener": {
        "protocol_port": 8000,
        "protocol": "TCP",
        "description": "",
        "client_ca_tls_container_ref": null,
        "default_tls_container_ref": null,
        "admin_state_up": true,
        "http2_enable": false,
        "loadbalancers": [
            {
                "id": "3d77894d-2ffe-4411-ac0a-0d57689779b8"
            }
        ],
        "tenant_id": "1867112d054b427e808cc6096d8193a1",
        "project_id": "1867112d054b427e808cc6096d8193a1",
        "sni_container_refs": [],
        "connection_limit": -1,
        "default_pool_id": "b7e53dbd-62ab-4505-a280-5c066078a5c9",
        "id": "09e64049-2ab0-4763-a8c5-f4207875dc3e",
        "tags": [],
        "name": "listener-2",
        "insert_headers":{
            "X-Forwarded-ELB-IP":true,
            "X-Forwarded-Host":true
        },
        "created_at": "2018-07-25T01:54:13",
        "updated_at": "2018-07-25T01:54:14"
    }
}
```

Status Code

For details, see **Status Codes**.

6.2.3 Querying Listeners

Function

This API is used to query the listeners and display them in a list. Filter query and pagination query are supported. Unless otherwise specified, exact match is applied.

You can query listeners using information such as listener ID, protocol used by the listener, port used by the listener, or backend server private IP address.

URI

GET /v2/{project_id}/elb/listeners

Table 6-54 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Table 6-55 Query parameters

Parameter	Mandatory	Type	Description
marker	No	String	Specifies the ID of the listener from which pagination query starts, that is, the ID of the last listener on the previous page. This parameter must be used together with **limit**.
limit	No	Integer	Specifies the number of listeners on each page. If this parameter is not set, all listeners are queried by default.
page_reverse	No	Boolean	Specifies the page direction. The value can be **true** or **false**, and the default value is **false**. The last page in the list requested with **page_reverse** set to **false** will not contain the "next" link, and the last page in the list requested with **page_reverse** set to **true** will not contain the "previous" link. This parameter must be used together with **limit**.
id	No	String	Specifies the listener ID.
name	No	String	Specifies the listener name. The value contains a maximum of 255 characters.
description	No	String	Provides supplementary information about the listener. The value contains a maximum of 255 characters.
loadbalancer_id	No	String	Specifies the ID of the associated load balancer.
connection_limit	No	Integer	Specifies the maximum number of connections.
admin_state_up	No	Boolean	Specifies the administrative status of the listener. This parameter is reserved, and the default value is **true**.

Parameter	Mandatory	Type	Description
default_pool_id	No	String	Specifies the ID of the associated backend server group. If a request does not match the forwarding policy, the request is forwarded to the default backend server group for processing.
http2_enable	No	Boolean	Specifies whether to use HTTP/2. The value can be **true** or **false**. • **true**: HTTP/2 is used. • **false**: HTTP/2 is not used.
default_tls_container_ref	No	String	Specifies the ID of the server certificate used by the listener.
client_ca_tls_container_ref	No	String	Specifies the ID of the CA certificate used by the listener.
protocol	No	String	Specifies the protocol used by the listener. The value can be **TCP**, **HTTP**, **UDP**, or **TERMINATED_HTTPS**.
protocol_port	No	Integer	Specifies the port used by the listener.
enterprise_project_id	No	String	Specifies the enterprise project ID. Enterprise projects are used for fine-grained authentication. • If **default_pool_id** is passed, the ID of the enterprise project to which the backend server group belongs is used for authentication. • If neither **default_pool_id** nor **enterprise_project_id** is passed, fine-grained authentication is performed. The **elb:*list** permissions must be assigned to the user group.

Parameter	Mandatory	Type	Description
tls_ciphers_policy	No	String	Specifies the security policy used by the listener. This parameter takes effect only when the protocol used by the listener is set to **TERMINATED_HTTPS**. The value can be **tls-1-0-inherit**, **tls-1-0**, **tls-1-1**, **tls-1-2**, or **tls-1-2-strict**, and the default value is **tls-1-0**. For details of cipher suites for each security policy, see **Table 6-56**.

Table 6-56 tls_ciphers_policy parameter description

Security Policy	TLS Version	Cipher Suite
tls-1-0-inherit	TLS 1.2 TLS 1.1 TLS 1.0	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:DHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:AES128-SHA:AES256-SHA:DHE-DSS-AES128-SHA:CAMELLIA128-SHA:EDH-RSA-DES-CBC3-SHA:DES-CBC3-SHA:ECDHE-RSA-RC4-SHA:RC4-SHA:DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:DHE-RSA-CAMELLIA256-SHA:DHE-DSS-CAMELLIA256-SHA:CAMELLIA256-SHA:EDH-DSS-DES-CBC3-SHA:DHE-RSA-CAMELLIA128-SHA:DHE-DSS-CAMELLIA128-SHA
tls-1-0	TLS 1.2 TLS 1.1 TLS 1.0	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:AES128-SHA:AES256-SHA
tls-1-1	TLS 1.2 TLS 1.1	
tls-1-2	TLS 1.2	

Security Policy	TLS Version	Cipher Suite
tls-1-2-strict	TLS 1.2	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384

Request

None

Response

Table 6-57 Response parameters

Parameter	Type	Description
listeners	Array of **Listeners** objects	Lists the listeners. For details, see **Table 6-58**.

Table 6-58 listener parameter description

Parameter	Type	Description
id	String	Specifies the listener ID.
tenant_id	String	Specifies the ID of the project where the listener is used. The value contains a maximum of 255 characters.
project_id	String	Specifies the ID of the project to which the listener belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the listener name. Note: If you leave the listener name empty, you cannot locate it on the listener list and view its details. The value contains a maximum of 255 characters.

Parameter	Type	Description
description	String	Provides supplementary information about the listener. The value contains a maximum of 255 characters.
protocol	String	Specifies the protocol used by the listener. The value can be **TCP**, **HTTP**, **UDP**, or **TERMINATED_HTTPS**.
protocol_port	Integer	Specifies the port used by the listener. The port number ranges from 1 to 65535.
loadbalancers	Array of **Loadbalancers** objects	Specifies the ID of the associated load balancer. For details, see **Table 6-45**.
connection_limit	Integer	Specifies the maximum number of connections. The value ranges from **-1** to **2147483647**. The default value is **-1**, indicating that there is no restriction on the maximum number of connections. This parameter is reserved.
admin_state_up	Boolean	Specifies the administrative status of the listener. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
http2_enable	Boolean	Specifies whether to use HTTP/2. The value can be **true** or **false**. • **true**: HTTP/2 is used. • **false**: HTTP/2 is not used. This parameter takes effect only when the protocol used by the listener is set to **TERMINATED_HTTPS**.
default_pool_id	String	Specifies the ID of the associated backend server group. If a request does not match the forwarding policy, the request is forwarded to the default backend server group for processing. If the value is **null**, the listener has no default backend server group.

Parameter	Type	Description
default_tls_container_ref	String	Specifies the ID of the server certificate used by the listener. For details, see **Certificate**. This parameter is mandatory when **protocol** is set to **TERMINATED_HTTPS**. The value contains a maximum of 128 characters.
client_ca_tls_container_ref	String	Specifies the ID of the CA certificate used by the listener. The value contains a maximum of 128 characters. For details, see **Certificate**.
sni_container_refs	Array	Lists the IDs of SNI certificates (server certificates with domain names) used by the listener. If the parameter value is an empty list, the SNI feature is disabled.
tags	Array	Tags the listener.
created_at	String	Specifies the time when the listener was created. YYYY-MM-DDTHH:MM:SS
updated_at	String	Specifies the time when the listener was updated. YYYY-MM-DDTHH:MM:SS
insert_headers	**InsertHeaders** object	Specifies whether to insert HTTP extension headers and sent them to backend servers. All headers are synchronized. If this parameter is not set, default values are used. Information required by backend servers can be written into HTTP headers and passed to backend servers. For example, you can use the **X-Forwarded-ELB-IP** header to transmit the load balancer EIP to backend servers. For details, see **Table 6-46**.
tls_ciphers_policy	String	Specifies the security policy used by the listener. This parameter takes effect only when the protocol used by the listener is set to **TERMINATED_HTTPS**. The value can be **tls-1-0-inherit**, **tls-1-0**, **tls-1-1**, **tls-1-2**, or **tls-1-2-strict**, and the default value is **tls-1-0**. Lists cipher suites used by each security policy. For details, see **Table 6-47**.

Parameter	Type	Description
protection_status	String	String Specifies whether modification protection is enabled. The value can be one of the following: • **nonProtection** (default): Modification protection is not enabled. • **consoleProtection**: Modification protection is enabled to avoid that resources are modified by accident on the console.
protection_reason	String	String Specifies the reason to enable modification protection. This parameter is valid only when **protection_status** is set to **consoleProtection**.

Table 6-59 loadbalancers parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	Specifies the ID of the associated load balancer.

Table 6-60 insert_headers parameter description

Parameter	Mandatory	Type	Description
X-Forwarded-ELB-IP	No	Boolean	Specifies whether to transparently transmit the load balancer EIP to backend servers. After this function is enabled, the load balancer EIP is stored in the HTTP header and passes to backend servers. The value can be **true** or **false**. **true**: This function is enabled. **false**: The function is disabled. The function is disabled by default.

Parameter	Mandatory	Type	Description
X-Forwarded-Host	No	Boolean	Specifies whether to rewrite the **X-Forwarded-Host** header. If this function is enabled, **X-Forwarded-Host** is rewritten based on **Host** in the request and sent to backend servers. The value can be **true** or **false**. **true**: This function is enabled. **false**: The function is disabled. The function is enabled by default.

Table 6-61 tls_ciphers_policy parameter description

Security Policy	TLS Version	Cipher Suite
tls-1-0-inherit	TLS 1.2 TLS 1.1 TLS 1.0	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:DHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:AES128-SHA:AES256-SHA:DHE-DSS-AES128-SHA:CAMELLIA128-SHA:EDH-RSA-DES-CBC3-SHA:DES-CBC3-SHA:ECDHE-RSA-RC4-SHA:RC4-SHA:DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:DHE-RSA-CAMELLIA256-SHA:DHE-DSS-CAMELLIA256-SHA:CAMELLIA256-SHA:EDH-DSS-DES-CBC3-SHA:DHE-RSA-CAMELLIA128-SHA:DHE-DSS-CAMELLIA128-SHA
tls-1-0	TLS 1.2 TLS 1.1 TLS 1.0	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:AES128-SHA:AES256-SHA
tls-1-1	TLS 1.2 TLS 1.1	
tls-1-2	TLS 1.2	

Security Policy	TLS Version	Cipher Suite
tls-1-2-strict	TLS 1.2	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384

Example Request

- Example request 1: Querying all listeners
  GET https://{Endpoint}/v2/601240b9c5c94059b63d484c92cfe308/elb/listeners
- Request example 2: Querying UDP listeners
  GET https://{Endpoint}/v2/601240b9c5c94059b63d484c92cfe308/elb/listeners?protocol=UDP

Example Response

- Example response 1

```
{
   "listeners": [
      {
         "client_ca_tls_container_ref": null,
         "protocol": "TCP",
         "description": "",
         "default_tls_container_ref": null,
         "admin_state_up": true,
         "http2_enable": false,
         "loadbalancers": [
            {
               "id": "bc7ba445-035a-4464-a1a3-a62cf4a14116"
            }
         ],
         "tenant_id": "601240b9c5c94059b63d484c92cfe308",
         "project_id": "601240b9c5c94059b63d484c92cfe308",
         "sni_container_refs": [],

         "connection_limit": -1,
         "protocol_port": 80,
         "default_pool_id": "ed75f16e-fcc6-403e-a3fb-4eae82005eab",
         "id": "75045172-70e9-480d-9443-b8b6459948f7",
         "tags": [],
         "name": "listener-cb2n",
         "insert_headers":{
            "X-Forwarded-ELB-IP":true,
            "X-Forwarded-Host":true
         },
         "created_at": "2018-07-25T01:54:13",
         "updated_at": "2018-07-25T01:54:14"
      },
      {
         "client_ca_tls_container_ref": null,
         "protocol": "TCP",
         "description": "",
         "default_tls_container_ref": null,
         "admin_state_up": true,
         "http2_enable": false,
         "loadbalancers": [
            {
```



```
                "id": "165b6a38-5278-4569-b747-b2ee65ea84a4"
            }
        ],
        "tenant_id": "601240b9c5c94059b63d484c92cfe308",
        "sni_container_refs": [],

        "connection_limit": -1,
        "protocol_port": 8080,
        "default_pool_id": null,
        "id": "dada0003-7b0e-4de8-a4e1-1e937be2ba14",
        "tags": [],
        "name": "lsnr_name_mod",
        "insert_headers":{
            "X-Forwarded-ELB-IP":true,
            "X-Forwarded-Host":true
        },
        "created_at": "2018-07-25T01:54:13",
        "updated_at": "2018-07-25T01:54:14"
    }
  ]
}
```


- Example response 2


```
{
  "listeners": [
    {
        "insert_headers": null,
        "protocol_port": 64809,
        "protocol": "UDP",
        "description": "",
        "default_tls_container_ref": null,
        "sni_container_refs": [],
        "loadbalancers": [
            {
                "id": "c1127125-64a9-4394-a08a-ef3be8f7ef9c"
            }
        ],
        "tenant_id": "601240b9c5c94059b63d484c92cfe308",
        "project_id": "601240b9c5c94059b63d484c92cfe308",
        "created_at": "2018-11-29T13:56:21",
        "client_ca_tls_container_ref": null,
        "connection_limit": -1,
        "updated_at": "2018-11-29T13:56:22",
        "http2_enable": false,
        "insert_headers":{
            "X-Forwarded-ELB-IP":true,
            "X-Forwarded-Host":true
        },

        "admin_state_up": true,
        "default_pool_id": "2f6895be-019b-4c82-9b53-c4a2ac009e20",
        "id": "5c63d176-444f-4c75-9cfe-bcb8a05a845c",
        "tags": [],
        "name": "listener-tvp8"
    }
  ]
}
```


Status Code

For details, see **Status Codes**.

6.2.4 Updating a Listener

Function

This API is used to update a listener, such as listener name, description, associated backend server groups, and server certificates.

Constraints

- If the provisioning status of the associated load balancer is not **ACTIVE**, the listener cannot be updated.
- Only users with the ELB administrator permissions can specify the value of **connection_limit**.
- The **default_pool_id** parameter has the following constraints:
  - Its value cannot be the ID of any backend server group of other listeners.
  - Its value cannot be the ID of any backend server group associated with the forwarding policies set for other listeners.
- The relationships between the protocol used by the listener and the protocol of the backend server group are as follows:
  - When the protocol used by the listener is **TCP**, the protocol of the backend server group must be **TCP**.
  - When the protocol used by the listener is **UDP**, the backend server group protocol must be **UDP**.
  - When the protocol used by the listener is **HTTP** or **TERMINATED_HTTPS**, the protocol of the backend server group must be **HTTP**.

URI

PUT /v2/{project_id}/elb/listeners/{listener_id}

Table 6-62 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
listener_id	Yes	String	Specifies the listener ID.

Request

Table 6-63 Parameter description

Parameter	Mandatory	Type	Description
listener	Yes	**Listener** object	Specifies the listener. For details, see **Table 6-64**.

Table 6-64 listener parameter description

Parameter	Mandatory	Type	Description
name	No	String	Specifies the listener name. Note: If you leave the listener name empty, you cannot locate it on the listener list and view its details. The value contains a maximum of 255 characters.
description	No	String	Provides supplementary information about the listener. The value contains a maximum of 255 characters.
connection_limit	No	Integer	Specifies the maximum number of connections. The value ranges from **-1** to **2147483647**. This field is reserved. Do not use it. Only users with the ELB administrator permissions can specify this field.
http2_enable	No	Boolean	Specifies whether to use HTTP/2. The value can be **true** or **false**. • **true**: HTTP/2 is used. • **false**: HTTP/2 is not used. This parameter takes effect only when the protocol used by the listener is set to **TERMINATED_HTTPS**.

Parameter	Mandatory	Type	Description
default_pool_id	No	String	Specifies the ID of the associated backend server group. If a request does not match the forwarding policy, the request is forwarded to the default backend server group for processing. If the value is **null**, the listener has no default backend server group. The **default_pool_id** parameter has the following constraints: • Its value cannot be the ID of any backend server group of other listeners. • Its value cannot be the ID of any backend server group associated with the forwarding policies set for other listeners. The relationships between the protocol of the backend server group and the protocol used by the listener are as follows: • When the protocol used by the listener is **TCP**, the protocol of the backend server group must be **TCP**. • When the protocol used by the listener is **UDP**, the protocol of the backend server group must be **UDP**. • When the protocol used by the listener is **HTTP** or **TERMINATED_HTTPS**, the protocol of the backend server group must be **HTTP**.
admin_state_up	No	Boolean	Specifies the administrative status of the listener. This parameter is reserved, and the default value is **true**.

Parameter	Mandatory	Type	Description
default_tls_container_ref	No	String	Specifies the ID of the server certificate used by the listener. The value contains a maximum of 128 characters. This parameter is mandatory when **protocol** is set to **TERMINATED_HTTPS**.
client_ca_tls_container_ref	No	String	Specifies the ID of the CA certificate used by the listener. The value contains a maximum of 128 characters.
sni_container_refs	No	Array	Lists the IDs of SNI certificates (server certificates with domain names) used by the listener. If the parameter value is an empty list, the SNI feature is disabled.
insert_headers	No	**InsertHeaders** object	Specifies whether to insert HTTP extension headers and sent them to backend servers. All headers are synchronized. If this parameter is not set, default values are used. Information required by backend servers can be written into HTTP headers and passed to backend servers. For example, you can use the **X-Forwarded-ELB-IP** header to transmit the load balancer EIP to backend servers. For details, see **Table 6-65**. **NOTE** This parameter takes effect only when the protocol used by the listener is set to **HTTP** or **TERMINATED_HTTPS**.

Parameter	Mandatory	Type	Description
tls_ciphers_policy	No	String	Specifies the security policy used by the listener. This parameter takes effect only when the protocol used by the listener is set to **TERMINATED_HTTPS**. The value can be **tls-1-0-inherit**, **tls-1-0**, **tls-1-1**, **tls-1-2**, or **tls-1-2-strict**, and the default value is **tls-1-0**. For details of cipher suites for each security policy, see **Table 6-66**.
protection_status	No	String	Specifies whether modification protection is enabled. The value can be one of the following: • **nonProtection** (default): Modification protection is not enabled. • **consoleProtection**: Modification protection is enabled to avoid that resources are modified by accident on the console.
protection_reason	No	String	Specifies the reason to enable modification protection. This parameter is valid only when **protection_status** is set to **consoleProtection**.

Table 6-65 insert_headers parameter description

Parameter	Mandatory	Type	Description
X-Forwarded-ELB-IP	No	Boolean	Specifies whether to transparently transmit the load balancer EIP to backend servers. After this function is enabled, the load balancer EIP is stored in the HTTP header and passes to backend servers. The value can be **true** or **false**. **true**: This function is enabled. **false**: The function is disabled. The function is disabled by default.

Parameter	Mandatory	Type	Description
X-Forwarded-Host	No	Boolean	Specifies whether to rewrite the **X-Forwarded-Host** header. If this function is enabled, **X-Forwarded-Host** is rewritten based on **Host** in the request and sent to backend servers. The value can be **true** or **false**. **true**: This function is enabled. **false**: The function is disabled. The function is enabled by default.

Table 6-66 tls_ciphers_policy parameter description

Security Policy	TLS Version	Cipher Suite
tls-1-0-inherit	TLS 1.2 TLS 1.1 TLS 1.0	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:DHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:AES128-SHA:AES256-SHA:DHE-DSS-AES128-SHA:CAMELLIA128-SHA:EDH-RSA-DES-CBC3-SHA:DES-CBC3-SHA:ECDHE-RSA-RC4-SHA:RC4-SHA:DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:DHE-RSA-CAMELLIA256-SHA:DHE-DSS-CAMELLIA256-SHA:CAMELLIA256-SHA:EDH-DSS-DES-CBC3-SHA:DHE-RSA-CAMELLIA128-SHA:DHE-DSS-CAMELLIA128-SHA
tls-1-0	TLS 1.2 TLS 1.1 TLS 1.0	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:AES128-SHA:AES256-SHA
tls-1-1	TLS 1.2 TLS 1.1	
tls-1-2	TLS 1.2	

Security Policy	TLS Version	Cipher Suite
tls-1-2-strict	TLS 1.2	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384

Response

Table 6-67 Response parameters

Parameter	Type	Description
listener	**Listener** object	Specifies the listener. For details, see **Table 6-68**.

Table 6-68 listener parameter description

Parameter	Type	Description
id	String	Specifies the listener ID.
tenant_id	String	Specifies the ID of the project where the listener is used. The value contains a maximum of 255 characters.
project_id	String	Specifies the ID of the project to which the listener belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the listener name. Note: If you leave the listener name empty, you cannot locate it on the listener list and view its details. The value contains a maximum of 255 characters.
description	String	Provides supplementary information about the listener. The value contains a maximum of 255 characters.

Parameter	Type	Description
protocol	String	Specifies the protocol used by the listener. The value can be **TCP**, **HTTP**, **UDP**, or **TERMINATED_HTTPS**.
protocol_port	Integer	Specifies the port used by the listener. The port number ranges from 1 to 65535.
loadbalancers	Array of **Loadbalancers** objects	Specifies the ID of the associated load balancer. For details, see **Table 6-45**.
connection_limit	Integer	Specifies the maximum number of connections. The value ranges from **-1** to **2147483647**. The default value is **-1**, indicating that there is no restriction on the maximum number of connections. This parameter is reserved.
admin_state_up	Boolean	Specifies the administrative status of the listener. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
http2_enable	Boolean	Specifies whether to use HTTP/2. The value can be **true** or **false**. • **true**: HTTP/2 is used. • **false**: HTTP/2 is not used. This parameter takes effect only when the protocol used by the listener is set to **TERMINATED_HTTPS**.
default_pool_id	String	Specifies the ID of the associated backend server group. If a request does not match the forwarding policy, the request is forwarded to the default backend server group for processing. If the value is **null**, the listener has no default backend server group.
default_tls_container_ref	String	Specifies the ID of the server certificate used by the listener. For details, see **Certificate**. This parameter is mandatory when **protocol** is set to **TERMINATED_HTTPS**. The value contains a maximum of 128 characters.

Parameter	Type	Description
client_ca_tls_container_ref	String	Specifies the ID of the CA certificate used by the listener. The value contains a maximum of 128 characters. For details, see **Certificate**.
sni_container_refs	Array	Lists the IDs of SNI certificates (server certificates with domain names) used by the listener. If the parameter value is an empty list, the SNI feature is disabled.
tags	Array	Tags the listener.
created_at	String	Specifies the time when the listener was created. YYYY-MM-DDTHH:MM:SS
updated_at	String	Specifies the time when the listener was updated. YYYY-MM-DDTHH:MM:SS
insert_headers	**InsertHeaders** object	Specifies whether to insert HTTP extension headers and sent them to backend servers. All headers are synchronized. If this parameter is not set, default values are used. Information required by backend servers can be written into HTTP headers and passed to backend servers. For example, you can use the **X-Forwarded-ELB-IP** header to transmit the load balancer EIP to backend servers. For details, see **Table 6-46**.
tls_ciphers_policy	String	Specifies the security policy used by the listener. This parameter takes effect only when the protocol used by the listener is set to **TERMINATED_HTTPS**. The value can be **tls-1-0-inherit**, **tls-1-0**, **tls-1-1**, **tls-1-2**, or **tls-1-2-strict**, and the default value is **tls-1-0**. Lists cipher suites used by each security policy. For details, see **Table 6-47**.

Parameter	Type	Description
protection_status	String	String Specifies whether modification protection is enabled. The value can be one of the following: • **nonProtection** (default): Modification protection is not enabled. • **consoleProtection**: Modification protection is enabled to avoid that resources are modified by accident on the console.
protection_reason	String	String Specifies the reason to enable modification protection. This parameter is valid only when **protection_status** is set to **consoleProtection**.

Table 6-69 loadbalancers parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	Specifies the ID of the associated load balancer.

Table 6-70 insert_headers parameter description

Parameter	Mandatory	Type	Description
X-Forwarded-ELB-IP	No	Boolean	Specifies whether to transparently transmit the load balancer EIP to backend servers. After this function is enabled, the load balancer EIP is stored in the HTTP header and passes to backend servers. The value can be **true** or **false**. **true**: This function is enabled. **false**: The function is disabled. The function is disabled by default.

Parameter	Mandatory	Type	Description
X-Forwarded-Host	No	Boolean	Specifies whether to rewrite the **X-Forwarded-Host** header. If this function is enabled, **X-Forwarded-Host** is rewritten based on **Host** in the request and sent to backend servers. The value can be **true** or **false**. **true**: This function is enabled. **false**: The function is disabled. The function is enabled by default.

Table 6-71 tls_ciphers_policy parameter description

Security Policy	TLS Version	Cipher Suite
tls-1-0-inherit	TLS 1.2 TLS 1.1 TLS 1.0	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:DHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:AES128-SHA:AES256-SHA:DHE-DSS-AES128-SHA:CAMELLIA128-SHA:EDH-RSA-DES-CBC3-SHA:DES-CBC3-SHA:ECDHE-RSA-RC4-SHA:RC4-SHA:DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:DHE-RSA-CAMELLIA256-SHA:DHE-DSS-CAMELLIA256-SHA:CAMELLIA256-SHA:EDH-DSS-DES-CBC3-SHA:DHE-RSA-CAMELLIA128-SHA:DHE-DSS-CAMELLIA128-SHA
tls-1-0	TLS 1.2 TLS 1.1 TLS 1.0	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:AES128-SHA:AES256-SHA
tls-1-1	TLS 1.2 TLS 1.1	
tls-1-2	TLS 1.2	

Security Policy	TLS Version	Cipher Suite
tls-1-2-strict	TLS 1.2	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384

Example Request

- Example request: Updating a listener

```
PUT https://{Endpoint}/v2/601240b9c5c94059b63d484c92cfe308/elb/listeners/f622c150-72f5-4263-a47a-e5003c652aa3
{
    "listener": {
        "description": "my listener",
        "name": "listener-jy-test2",
        "default_tls_container_ref": "23b58a961a4d4c95be585e98046e657a",
        "client_ca_tls_container_ref": "417a0976969f497db8cbb083bff343ba",
        "default_pool_id": "c61310de-9a06-4f0c-850c-6f4797b9984c"
    }
}
```

Example Response

- Example response

```
{
    "listener": {
        "client_ca_tls_container_ref": "417a0976969f497db8cbb083bff343ba",
        "protocol": "TERMINATED_HTTPS",
        "description": "my listener",
        "default_tls_container_ref": "23b58a961a4d4c95be585e98046e657a",
        "admin_state_up": true,
        "http2_enable": false,
        "loadbalancers": [
            {
                "id": "165b6a38-5278-4569-b747-b2ee65ea84a4"
            }
        ],
        "tenant_id": "601240b9c5c94059b63d484c92cfe308",
        "project_id": "601240b9c5c94059b63d484c92cfe308",
        "sni_container_refs": [],
        "connection_limit": -1,
        "protocol_port": 443,
        "tags": [],
        "default_pool_id": "c61310de-9a06-4f0c-850c-6f4797b9984c",
        "id": "f622c150-72f5-4263-a47a-e5003c652aa3",
        "name": "listener-jy-test2",
            "insert_headers":{
                "X-Forwarded-ELB-IP":true,
                "X-Forwarded-Host":true
            },
        "created_at": "2018-07-25T01:54:13",
        "updated_at": "2018-07-25T01:54:14"
    }
}
```


Status Code

For details, see **Status Codes**.

6.2.5 Deleting a Listener

Function

This API is used to delete a listener by ID.

Constraints

If the **cascade** value is **false**, delete the associated backend server groups by referring to **Deleting a Backend Server Group**, or change the value of **default_pool_id** to **null** by referring to **Updating a Listener** and delete associated forwarding policies by referring to **Deleting a Forwarding Policy**, before attempting to delete the listener.

URI

DELETE /v2/{project_id}/elb/listeners/{listener_id}

Table 6-72 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
listener_id	Yes	String	Specifies the listener ID.
cascade	No	Boolean	Specifies whether to delete the resources associated with the listener when it is deleted, including forwarding policy and backend servers.

Request

None

Response

None

Example Request

- Example request: Deleting a listener
  DELETE https://{Endpoint}/v2/{project_id}/elb/listeners/35cb8516-1173-4035-8dae-0dae3453f37f

Example Response

- Example response

  None

Status Code

For details, see **Status Codes**.

6.3 Backend Server Group

6.3.1 Adding a Backend Server Group

Function

This API is used to add a backend server group. After multiple backend servers are added to a backend server group, requests are distributed among backend servers based on the load balancing algorithm configured for the backend server group and the weight set for each backend server.

Constraints

- If parameter **session-persistence** is configured, parameter **cookie_name** is available only when the value of **type** is **APP_COOKIE**.

URI

POST /v2/{project_id}/elb/pools

Table 6-73 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Request

Table 6-74 Parameter description

Parameter	Mandatory	Type	Description
pool	Yes	**Pool** object	Specifies the backend server group. For details, see **Table 6-75**.

Table 6-75 pool parameter description

Parameter	Mandatory	Type	Description
tenant_id	No	String	Specifies the ID of the project where the backend server group is used. The value must be the same as the value of **project_id** in the token. The value contains a maximum of 255 characters.
name	No	String	Specifies the name of the backend server group. The value contains a maximum of 255 characters.
description	No	String	Provides supplementary information about the backend server group. The value contains a maximum of 255 characters.
protocol	Yes	String	Specifies the protocol that the backend server group uses to receive requests. TCP, UDP, and HTTP are supported. When a backend server group is associated with a listener, the relationships between the protocol used by the listener and the protocol of the backend server group are as follows: ● When the protocol used by the listener is **UDP**, the protocol of the backend server group must be **UDP**. ● When the protocol used by the listener is **TCP**, the protocol of the backend server group must be **TCP**. ● When the protocol used by the listener is **HTTP** or **TERMINATED_HTTPS**, the protocol of the backend server group must be **HTTP**.

Parameter	Mandatory	Type	Description
lb_algorithm	Yes	String	Specifies the load balancing algorithm of the backend server group. The value can be: • **ROUND_ROBIN**: indicates the weighted round robin algorithm. • **LEAST_CONNECTIONS**: indicates the weighted least connections algorithm. • **SOURCE_IP**: indicates the source IP hash algorithm. When the value is **SOURCE_IP**, the weights of backend servers in the server group are invalid.
admin_state_up	No	Boolean	Specifies the administrative status of the backend server group. This parameter is reserved, and the default value is **true**.
listener_id	No	String	Specifies the ID of the listener associated with the backend server group. Specify either **listener_id** or **loadbalancer_id**, or both of them.
loadbalancer_id	No	String	Specifies the ID of the load balancer associated with the backend server group. Specify either **listener_id** or **loadbalancer_id**, or both of them.
session_persistence	No	**SessionPersistence** object	Specifies the sticky session timeout duration in minutes. For details, see **Table 6-76**. If the value is **null**, the sticky session feature is disabled.

Parameter	Mandatory	Type	Description
protection_status	No	String	Specifies whether modification protection is enabled. The value can be one of the following: • **nonProtection** (default): Modification protection is not enabled. • **consoleProtection**: Modification protection is enabled to avoid that resources are modified by accident on the console.
protection_reason	No	String	Specifies the reason to enable modification protection. This parameter is valid only when **protection_status** is set to **consoleProtection**.

Table 6-76 session_persistence parameter description

Parameter	Mandatory	Type	Description
type	Yes	String	Specifies the sticky session type. The value can be: • **SOURCE_IP**: Requests are distributed based on the client's IP address. Requests from the same IP address are sent to the same backend server. • **HTTP_COOKIE**: When the client sends a request for the first time, the load balancer automatically generates a cookie and inserts the cookie into the response message. Subsequent requests are sent to the backend server that processes the first request. • **APP_COOKIE**: When the client sends a request for the first time, the backend server that receives the request generates a cookie and inserts the cookie into the response message. Subsequent requests are sent to this backend server. When the protocol of the backend server group is TCP, only **SOURCE_IP** takes effect. When the protocol of the backend server group is HTTP, only **HTTP_COOKIE** or **APP_COOKIE** takes effect.
cookie_name	No	String	Specifies the cookie name. The name can contain up to 64 characters, including letters, digits, hyphens (-), and underscores (_). This parameter is mandatory when the sticky session type is **APP_COOKIE**.

Parameter	Mandatory	Type	Description
persistence_timeout	No	Integer	Specifies the sticky session timeout duration in minutes. This parameter is invalid when **type** is set to **APP_COOKIE**. The value range varies depending on the protocol of the backend server group: • When the protocol of the backend server group is TCP or UDP, the value ranges from **1** to **60**. • When the protocol of the backend server group is HTTP or HTTPS, the value ranges from **1** to **1440**.

Response

Table 6-77 Parameter description

Parameter	Type	Description
pool	**Pool** object	Specifies the backend server group. For details, see **Table 6-78**.

Table 6-78 pool parameter description

Parameter	Type	Description
id	String	Specifies the ID of the backend server group.
tenant_id	String	Specifies the ID of the project where the backend server group is used. The value contains a maximum of 255 characters.
project_id	String	Specifies the ID of the project to which the backend server group belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the name of the backend server group. The value contains a maximum of 255 characters.

Parameter	Type	Description
description	String	Provides supplementary information about the backend server group. The value contains a maximum of 255 characters.
protocol	String	Specifies the protocol that the backend server group uses to receive requests. TCP, UDP, and HTTP are supported. When a backend server group is associated with a listener, the relationships between the protocol used by the listener and the protocol of the backend server group are as follows: • When the protocol used by the listener is **UDP**, the protocol of the backend server group must be **UDP**. • When the protocol used by the listener is **TCP**, the protocol of the backend server group must be **TCP**. • When the protocol used by the listener is **HTTP** or **TERMINATED_HTTPS**, the protocol of the backend server group must be **HTTP**.
lb_algorithm	String	Specifies the load balancing algorithm of the backend server group. The value range varies depending on the protocol of the backend server group: • **ROUND_ROBIN**: indicates the weighted round robin algorithm. • **LEAST_CONNECTIONS**: indicates the weighted least connections algorithm. • **SOURCE_IP**: indicates the source IP hash algorithm. When the value is **SOURCE_IP**, the weights of backend servers in the server group are invalid.
members	Array of **Members** objects	Lists the IDs of backend servers in the backend server group. For details, see **Table 6-79**.
healthmonitor_id	String	Specifies the ID of the health check configured for the backend server group.

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the backend server group. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
listeners	Array of **Listeners** objects	Lists the IDs of listeners associated with the backend server group. For details, see **Table 6-80**.
loadbalancers	Array of **Loadbalancers** objects	Lists the IDs of load balancers associated with the backend server group. For details, see **Table 6-81**.
session_persistence	**SessionPersistence** object	Specifies whether to enable the sticky session feature. For details, see **Table 6-82**. Once sticky session are enabled, requests from the same client are sent to the same backend server during the session. When sticky sessions are disabled, the value is **null**.
protection_status	String	String Specifies whether modification protection is enabled. The value can be one of the following: • **nonProtection** (default): Modification protection is not enabled. • **consoleProtection**: Modification protection is enabled to avoid that resources are modified by accident on the console.
protection_reason	String	String Specifies the reason to enable modification protection. This parameter is valid only when **protection_status** is set to **consoleProtection**.

Table 6-79 members parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated backend server.

Table 6-80 listeners parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated backend server group.

Table 6-81 loadbalancers parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated load balancer.

Table 6-82 session_persistence parameter description

Parameter	Mandatory	Type	Description
type	Yes	String	Specifies the sticky session type. The value can be: • **SOURCE_IP**: Requests are distributed based on the client's IP address. Requests from the same IP address are sent to the same backend server. • **HTTP_COOKIE**: When the client sends a request for the first time, the load balancer automatically generates a cookie and inserts the cookie into the response message. Subsequent requests are sent to the backend server that processes the first request. • **APP_COOKIE**: When the client sends a request for the first time, the backend server that receives the request generates a cookie and inserts the cookie into the response message. Subsequent requests are sent to this backend server. When the protocol of the backend server group is TCP, only **SOURCE_IP** takes effect. When the protocol of the backend server group is HTTP, only **HTTP_COOKIE** or **APP_COOKIE** takes effect.

Parameter	Mandatory	Type	Description
cookie_name	No	String	Specifies the cookie name. The name can contain up to 64 characters, including letters, digits, hyphens (-), and underscores (_). This parameter is mandatory when the sticky session type is **APP_COOKIE**.
persistence_timeout	No	Integer	Specifies the sticky session timeout duration in minutes. This parameter is invalid when **type** is set to **APP_COOKIE**. The value range varies depending on the protocol of the backend server group: • When the protocol of the backend server group is TCP or UDP, the value ranges from **1** to **60**. • When the protocol of the backend server group is HTTP or HTTPS, the value ranges from **1** to **1440**.

Example Request

- Example request 1: Adding an HTTP backend server group

```
POST https://{Endpoint}/v2/601240b9c5c94059b63d484c92cfe308/elb/pools

{
    "pool": {
        "lb_algorithm":"ROUND_ROBIN",
        "loadbalancer_id": "63ad9dfe-4750-479f-9630-ada43ccc8117",
        "protocol":"HTTP"
    }
}
```

- Example request 2: Adding a backend server group with the value of **type** set to **APP_COOKIE**

```
POST https://{Endpoint}/v2/145483a5107745e9b3d80f956713e6a3/elb/pools

{
  "pool": {
    "lb_algorithm": "ROUND_ROBIN",
    "loadbalancer_id": "370fb112-e920-486a-b051-1d0d30704dd3",
    "protocol": "HTTP",
    "session_persistence": {
      "cookie_name": "my_cookie",
      "type": "APP_COOKIE",
      "persistence_timeout": 1
    },
    "admin_state_up": true
  }
}
```

- Example request 3: Adding an HTTP backend server group with the value of **type** set to **HTTP_COOKIE**


```
POST https://{Endpoint}/v2/601240b9c5c94059b63d484c92cfe308/elb/pools

{
    "pool": {
        "lb_algorithm":"ROUND_ROBIN",
        "loadbalancer_id": "63ad9dfe-4750-479f-9630-ada43ccc8117",
        "protocol":"HTTP",
        "session_persistence":{
            "type":"HTTP_COOKIE"
        }
    }
}
```

Example Response

- Example response 1

```
{
    "pool": {
        "lb_algorithm": "ROUND_ROBIN",
        "protocol": "HTTP",
        "description": "",
        "admin_state_up": true,
        "loadbalancers": [
            {
                "id": "63ad9dfe-4750-479f-9630-ada43ccc8117"
            }
        ],
        "tenant_id": "601240b9c5c94059b63d484c92cfe308",
        "project_id": "601240b9c5c94059b63d484c92cfe308",
        "session_persistence": null,
        "healthmonitor_id": null,
        "listeners": [],
        "members": [],
        "id": "4e496951-befb-47bf-9573-c1cd11825c07",
        "name": ""
    }
}
```

- Example response 2

```
{
  "pool": {
    "lb_algorithm": "ROUND_ROBIN",
    "protocol": "HTTP",
    "description": "",
    "admin_state_up": true,
    "loadbalancers": [
      {
        "id": "6b041b9e-976b-40ba-b075-375be6110b53"
      }
    ],
    "tenant_id": "145483a5107745e9b3d80f956713e6a3",
    "project_id": "145483a5107745e9b3d80f956713e6a3",
    "session_persistence": {
      "cookie_name": "my_cookie",
      "type": "APP_COOKIE",
      "persistence_timeout": 1
    },
    "healthmonitor_id": null,
    "listeners": [
      {
        "id": "370fb112-e920-486a-b051-1d0d30704dd3"
      }
    ],
    "members": [],
    "id": "307f8968-9474-4d0c-8434-66be09dabcc1",
    "name": ""
  }
}
```


- Example response 3

```
{
    "pool": {
        "lb_algorithm": "ROUND_ROBIN",
        "protocol": "HTTP",
        "description": "",
        "admin_state_up": true,
        "loadbalancers": [
            {
                "id": "63ad9dfe-4750-479f-9630-ada43ccc8117"
            }
        ],
        "tenant_id": "601240b9c5c94059b63d484c92cfe308",
        "project_id": "601240b9c5c94059b63d484c92cfe308",
        "session_persistence": {
            "persistence_timeout": 1440,
            "cookie_name": null,
            "type": "HTTP_COOKIE"
        },
        "healthmonitor_id": null,
        "listeners": [],
        "members": [],
        "id": "d46eab56-d76b-4cd3-8952-3c3c4cf113aa",
        "name": ""
    }
}
```

Status Code

For details, see **Status Codes**.

6.3.2 Querying Backend Server Groups

Function

This API is used to query the backend server groups and display them in a list. Filter query and pagination query are supported. Unless otherwise specified, exact match is applied.

URI

GET /v2/{project_id}/elb/pools

Table 6-83 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Table 6-84 Query parameters

Parameter	Mandatory	Type	Description
marker	No	String	Specifies the ID of the backend server group from which pagination query starts, that is, the ID of the last backend server group on the previous page. If this parameter is not specified, the first page will be queried. This parameter must be used together with **limit**.
limit	No	Integer	Specifies the number of backend server groups on each page. If this parameter is not set, all backend server groups are queried by default.
page_reverse	No	Boolean	Specifies the page direction. The value can be **true** or **false**, and the default value is **false**. The last page in the list requested with **page_reverse** set to **false** will not contain the "next" link, and the last page in the list requested with **page_reverse** set to **true** will not contain the "previous" link. This parameter must be used together with **limit**.
id	No	String	Specifies the ID of the backend server group.
name	No	String	Specifies the name of the backend server group. The value contains a maximum of 255 characters.
description	No	String	Provides supplementary information about the backend server group. The value contains a maximum of 255 characters.
healthmonitor_id	No	String	Specifies the ID of the health check configured for the backend server group.
loadbalancer_id	No	String	Specifies the ID of the load balancer associated with the backend server group.

Parameter	Mandatory	Type	Description
protocol	No	String	Specifies the protocol that the backend server group uses to receive requests. TCP, UDP, and HTTP are supported.
lb_algorithm	No	String	Specifies the load balancing algorithm of the backend server group. The value can be: • **ROUND_ROBIN**: indicates the weighted round robin algorithm. • **LEAST_CONNECTIONS**: indicates the weighted least connections algorithm. • **SOURCE_IP**: indicates the source IP hash algorithm. When the value is **SOURCE_IP**, the weights of backend servers in the server group are invalid. For details about parameter **weight**, see **Response**.
member_address	No	String	Lists the IDs of backend servers in the backend server group.
member_device_id	No	String	Specifies the ID of the cloud server used as the backend server in the backend server group.

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Specifies the enterprise project ID. Enterprise projects are used for fine-grained authentication. • If **loadbalancer_id** is passed, the ID of the enterprise project to which the load balancer belongs is used for authentication. • If **loadbalancer_id** is not passed but **healthmonitor_id** is passed, the ID of the enterprise project to which the load balancer belongs is used for authentication. • If any of the three parameters **enterprise_project_id**, **loadbalancer_id**, or **healthmonitor_id** is not passed, fine-grained authentication is performed. The **elb:loadbalancers:list** permissions must be assigned to the user group.

Request

None

Response

Table 6-85 Parameter description

Parameter	Type	Description
pools	Array of **Pools** objects	Specifies the backend server group. For details, see **Table 6-86**.

Table 6-86 pool parameter description

Parameter	Type	Description
id	String	Specifies the ID of the backend server group.

Parameter	Type	Description
tenant_id	String	Specifies the ID of the project where the backend server group is used. The value contains a maximum of 255 characters.
project_id	String	Specifies the ID of the project to which the backend server group belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the name of the backend server group. The value contains a maximum of 255 characters.
description	String	Provides supplementary information about the backend server group. The value contains a maximum of 255 characters.
protocol	String	Specifies the protocol that the backend server group uses to receive requests. TCP, UDP, and HTTP are supported. When a backend server group is associated with a listener, the relationships between the protocol used by the listener and the protocol of the backend server group are as follows: • When the protocol used by the listener is **UDP**, the protocol of the backend server group must be **UDP**. • When the protocol used by the listener is **TCP**, the protocol of the backend server group must be **TCP**. • When the protocol used by the listener is **HTTP** or **TERMINATED_HTTPS**, the protocol of the backend server group must be **HTTP**.

Parameter	Type	Description
lb_algorithm	String	Specifies the load balancing algorithm of the backend server group. The value range varies depending on the protocol of the backend server group: • **ROUND_ROBIN**: indicates the weighted round robin algorithm. • **LEAST_CONNECTIONS**: indicates the weighted least connections algorithm. • **SOURCE_IP**: indicates the source IP hash algorithm. When the value is **SOURCE_IP**, the weights of backend servers in the server group are invalid.
members	Array of **Members** objects	Lists the IDs of backend servers in the backend server group. For details, see **Table 6-79**.
healthmonitor_id	String	Specifies the ID of the health check configured for the backend server group.
admin_state_up	Boolean	Specifies the administrative status of the backend server group. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
listeners	Array of **Listeners** objects	Lists the IDs of listeners associated with the backend server group. For details, see **Table 6-80**.
loadbalancers	Array of **Loadbalancers** objects	Lists the IDs of load balancers associated with the backend server group. For details, see **Table 6-81**.
session_persistence	**SessionPersistence** object	Specifies whether to enable the sticky session feature. For details, see **Table 6-82**. Once sticky session are enabled, requests from the same client are sent to the same backend server during the session. When sticky sessions are disabled, the value is **null**.

Parameter	Type	Description
protection_status	String	String Specifies whether modification protection is enabled. The value can be one of the following: • **nonProtection** (default): Modification protection is not enabled. • **consoleProtection**: Modification protection is enabled to avoid that resources are modified by accident on the console.
protection_reason	String	String Specifies the reason to enable modification protection. This parameter is valid only when **protection_status** is set to **consoleProtection**.

Table 6-87 members parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated backend server.

Table 6-88 listeners parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated backend server group.

Table 6-89 loadbalancers parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated load balancer.

Table 6-90 session_persistence parameter description

Parameter	Mandatory	Type	Description
type	Yes	String	Specifies the sticky session type. The value can be: • **SOURCE_IP**: Requests are distributed based on the client's IP address. Requests from the same IP address are sent to the same backend server. • **HTTP_COOKIE**: When the client sends a request for the first time, the load balancer automatically generates a cookie and inserts the cookie into the response message. Subsequent requests are sent to the backend server that processes the first request. • **APP_COOKIE**: When the client sends a request for the first time, the backend server that receives the request generates a cookie and inserts the cookie into the response message. Subsequent requests are sent to this backend server. When the protocol of the backend server group is TCP, only **SOURCE_IP** takes effect. When the protocol of the backend server group is HTTP, only **HTTP_COOKIE** or **APP_COOKIE** takes effect.
cookie_name	No	String	Specifies the cookie name. The name can contain up to 64 characters, including letters, digits, hyphens (-), and underscores (_). This parameter is mandatory when the sticky session type is **APP_COOKIE**.

Parameter	Mandatory	Type	Description
persistence_timeout	No	Integer	Specifies the sticky session timeout duration in minutes. This parameter is invalid when **type** is set to **APP_COOKIE**. The value range varies depending on the protocol of the backend server group: • When the protocol of the backend server group is TCP or UDP, the value ranges from **1** to **60**. • When the protocol of the backend server group is HTTP or HTTPS, the value ranges from **1** to **1440**.

Example Request

- Example request 1: Querying all backend server groups
  ```
  GET https://{Endpoint}/v2/1867112d054b427e808cc6096d8193a1/elb/pools
  ```
- Example request 2: Querying backend server groups whose load balancing algorithm is **SOURCE_IP**
  ```
  GET https://{Endpoint}/v2/1867112d054b427e808cc6096d8193a1/elb/pools?lb_algorithm=SOURCE_IP
  ```

Example Response

- Example response 1
  ```
  {
     "pools": [
        {
           "lb_algorithm": "SOURCE_IP",
           "protocol": "TCP",
           "description": "",
           "admin_state_up": true,
           "loadbalancers": [
              {
                 "id": "07d28d4a-4899-40a3-a939-5d09d69019e1"
              }
           ],
           "tenant_id": "1867112d054b427e808cc6096d8193a1",
           "project_id": "1867112d054b427e808cc6096d8193a1",
           "session_persistence": null,
           "healthmonitor_id": null,
           "listeners": [
              {
                 "id": "1b421c2d-7e78-4a78-9ee4-c8ccba41f15b"
              }
           ],
           "members": [
              {
                 "id": "88f9c079-29cb-435a-b98f-0c5c0b90c2bd"
              },
              {
                 "id": "2f4c9644-d5d2-4cf8-a3c0-944239a4f58c"
              }
           ],
           "id": "3a9f50bb-f041-4eac-a117-82472d8a0007",
  ```



```
        "name": "my-pool"
      }
   ]
}
```


- Example response 2


```
{
   "pools": [
      {
         "lb_algorithm": "SOURCE_IP",
         "protocol": "TCP",
         "description": "",
         "admin_state_up": true,
         "loadbalancers": [
            {
               "id": "07d28d4a-4899-40a3-a939-5d09d69019e1"
            }
         ],
         "tenant_id": "1867112d054b427e808cc6096d8193a1",
         "project_id": "1867112d054b427e808cc6096d8193a1",
         "session_persistence": null,
         "healthmonitor_id": null,
         "listeners": [
            {
               "id": "1b421c2d-7e78-4a78-9ee4-c8ccba41f15b"
            }
         ],
         "members": [
            {
               "id": "88f9c079-29cb-435a-b98f-0c5c0b90c2bd"
            },
            {
               "id": "2f4c9644-d5d2-4cf8-a3c0-944239a4f58c"
            }
         ],
         "id": "3a9f50bb-f041-4eac-a117-82472d8a0007",
         "name": "my-pool"
      }
   ]
}
```


Status Code

For details, see **Status Codes**.

6.3.3 Querying Details of a Backend Server Group

Function

This API is used to query details about a backend server group using its ID.

URI

GET /v2/{project_id}/elb/pools/{pool_id}

Table 6-91 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Parameter	Mandatory	Type	Description
pool_id	Yes	String	Specifies the ID of the backend server group.

Request

None

Response

Table 6-92 Response parameters

Parameter	Type	Description
pool	**Pool** object	Specifies the backend server group. For details, see **Table 6-93**.

Table 6-93 pool parameter description

Parameter	Type	Description
id	String	Specifies the ID of the backend server group.
tenant_id	String	Specifies the ID of the project where the backend server group is used. The value contains a maximum of 255 characters.
project_id	String	Specifies the ID of the project to which the backend server group belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the name of the backend server group. The value contains a maximum of 255 characters.
description	String	Provides supplementary information about the backend server group. The value contains a maximum of 255 characters.

Parameter	Type	Description
protocol	String	Specifies the protocol that the backend server group uses to receive requests. TCP, UDP, and HTTP are supported. When a backend server group is associated with a listener, the relationships between the protocol used by the listener and the protocol of the backend server group are as follows: • When the protocol used by the listener is **UDP**, the protocol of the backend server group must be **UDP**. • When the protocol used by the listener is **TCP**, the protocol of the backend server group must be **TCP**. • When the protocol used by the listener is **HTTP** or **TERMINATED_HTTPS**, the protocol of the backend server group must be **HTTP**.
lb_algorithm	String	Specifies the load balancing algorithm of the backend server group. The value range varies depending on the protocol of the backend server group: • **ROUND_ROBIN**: indicates the weighted round robin algorithm. • **LEAST_CONNECTIONS**: indicates the weighted least connections algorithm. • **SOURCE_IP**: indicates the source IP hash algorithm. When the value is **SOURCE_IP**, the weights of backend servers in the server group are invalid.
members	Array of **Members** objects	Lists the IDs of backend servers in the backend server group. For details, see **Table 6-79**.
healthmonitor_id	String	Specifies the ID of the health check configured for the backend server group.
admin_state_up	Boolean	Specifies the administrative status of the backend server group. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled

Parameter	Type	Description
listeners	Array of **Listeners** objects	Lists the IDs of listeners associated with the backend server group. For details, see **Table 6-80**.
loadbalancers	Array of **Loadbalancers** objects	Lists the IDs of load balancers associated with the backend server group. For details, see **Table 6-81**.
session_persistence	**SessionPersistence** object	Specifies whether to enable the sticky session feature. For details, see **Table 6-82**. Once sticky session are enabled, requests from the same client are sent to the same backend server during the session. When sticky sessions are disabled, the value is **null**.
protection_status	String	String Specifies whether modification protection is enabled. The value can be one of the following: • **nonProtection** (default): Modification protection is not enabled. • **consoleProtection**: Modification protection is enabled to avoid that resources are modified by accident on the console.
protection_reason	String	String Specifies the reason to enable modification protection. This parameter is valid only when **protection_status** is set to **consoleProtection**.

Table 6-94 members parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated backend server.

Table 6-95 listeners parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated backend server group.

Table 6-96 loadbalancers parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated load balancer.

Table 6-97 session_persistence parameter description

Parameter	Mandatory	Type	Description
type	Yes	String	Specifies the sticky session type. The value can be: • **SOURCE_IP**: Requests are distributed based on the client's IP address. Requests from the same IP address are sent to the same backend server. • **HTTP_COOKIE**: When the client sends a request for the first time, the load balancer automatically generates a cookie and inserts the cookie into the response message. Subsequent requests are sent to the backend server that processes the first request. • **APP_COOKIE**: When the client sends a request for the first time, the backend server that receives the request generates a cookie and inserts the cookie into the response message. Subsequent requests are sent to this backend server. When the protocol of the backend server group is TCP, only **SOURCE_IP** takes effect. When the protocol of the backend server group is HTTP, only **HTTP_COOKIE** or **APP_COOKIE** takes effect.
cookie_name	No	String	Specifies the cookie name. The name can contain up to 64 characters, including letters, digits, hyphens (-), and underscores (_). This parameter is mandatory when the sticky session type is **APP_COOKIE**.

Parameter	Mandatory	Type	Description
persistence_timeout	No	Integer	Specifies the sticky session timeout duration in minutes. This parameter is invalid when **type** is set to **APP_COOKIE**. The value range varies depending on the protocol of the backend server group: • When the protocol of the backend server group is TCP or UDP, the value ranges from **1** to **60**. • When the protocol of the backend server group is HTTP or HTTPS, the value ranges from **1** to **1440**.

Example Request

- Example request: Querying details of a backend server group

```
GET https://{Endpoint}/v2/1867112d054b427e808cc6096d8193a1/elb/pools/5a9a3e9e-d1aa-448e-af37-a70171f2a332
```

Example Response

- Example response 1

```
{
    "pool": {
        "lb_algorithm": "SOURCE_IP",
        "protocol": "TCP",
        "description": "",
        "admin_state_up": true,
        "loadbalancers": [
            {
                "id": "6f52004c-3fe9-4c09-b8ce-ed9d9c74a3b1"
            }
        ],
        "tenant_id": "1867112d054b427e808cc6096d8193a1",
        "project_id": "1867112d054b427e808cc6096d8193a1",
        "session_persistence": null,
        "healthmonitor_id": null,
        "listeners": [
            {
                "id": "6e29b2cd-4e53-40f6-ae7b-29e918de67f2"
            }
        ],
        "members": [],
        "id": "5a9a3e9e-d1aa-448e-af37-a70171f2a332",
        "name": "my-pool"
    }
}
```

Status Code

For details, see **Status Codes**.

6.3.4 Updating a Backend Server Group

Function

This API is used to update a backend server group.

Constraints

If the provisioning status of the load balancer associated with a backend server group is not **ACTIVE**, the backend server group cannot be updated.

URI

PUT /v2/{project_id}/elb/pools/{pool_id}

Table 6-98 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
pool_id	Yes	String	Specifies the ID of the backend server group.

Request

Table 6-99 Parameter description

Parameter	Mandatory	Type	Description
pool	Yes	**Pool** object	Specifies the backend server group. For details, see **Table 6-100**.

Table 6-100 pool parameter description

Parameter	Mandatory	Type	Description
name	No	String	Specifies the name of the backend server group. The value contains a maximum of 255 characters.

Parameter	Mandatory	Type	Description
description	No	String	Provides supplementary information about the backend server group. The value contains a maximum of 255 characters.
lb_algorithm	No	String	Specifies the load balancing algorithm of the backend server group. The value can be: • **ROUND_ROBIN**: indicates the weighted round robin algorithm. • **LEAST_CONNECTIONS**: indicates the weighted least connections algorithm. • **SOURCE_IP**: indicates the source IP hash algorithm. When the value is **SOURCE_IP**, the weights of backend servers in the server group are invalid.
admin_state_up	No	Boolean	Specifies the administrative status of the backend server group. This parameter is reserved, and the default value is **true**.
session_persistence	No	**SessionPersistence** object	Specifies whether to enable the sticky session feature. For details, see **Table 6-101**. Once sticky session are enabled, requests from the same client are sent to the same backend server during the session. When sticky sessions are disabled, the value is **null**.

Parameter	Mandatory	Type	Description
protection_status	No	String	Specifies whether modification protection is enabled. The value can be one of the following: • **nonProtection** (default): Modification protection is not enabled. • **consoleProtection**: Modification protection is enabled to avoid that resources are modified by accident on the console.
protection_reason	No	String	Specifies the reason to enable modification protection. This parameter is valid only when **protection_status** is set to **consoleProtection**.

Table 6-101 session_persistence parameter description

Parameter	Mandatory	Type	Description
type	Yes	String	Specifies the sticky session type. The value can be: • **SOURCE_IP**: Requests are distributed based on the client's IP address. Requests from the same IP address are sent to the same backend server. • **HTTP_COOKIE**: When the client sends a request for the first time, the load balancer automatically generates a cookie and inserts the cookie into the response message. Subsequent requests are sent to the backend server that processes the first request. • **APP_COOKIE**: When the client sends a request for the first time, the backend server that receives the request generates a cookie and inserts the cookie into the response message. Subsequent requests are sent to this backend server. When the protocol of the backend server group is TCP, only **SOURCE_IP** takes effect. When the protocol of the backend server group is HTTP, only **HTTP_COOKIE** or **APP_COOKIE** takes effect.
cookie_name	No	String	Specifies the cookie name. The name can contain up to 64 characters, including letters, digits, hyphens (-), and underscores (_). This parameter is mandatory when the sticky session type is **APP_COOKIE**.

Parameter	Mandatory	Type	Description
persistence_timeout	No	Integer	Specifies the sticky session timeout duration in minutes. This parameter is invalid when **type** is set to **APP_COOKIE**. The value range varies depending on the protocol of the backend server group: • When the protocol of the backend server group is TCP or UDP, the value ranges from **1** to **60**. • When the protocol of the backend server group is HTTP or HTTPS, the value ranges from **1** to **1440**.

Response

Table 6-102 Response parameters

Parameter	Type	Description
pool	**Pool** object	Specifies the backend server group. For details, see **Table 6-103**.

Table 6-103 pool parameter description

Parameter	Type	Description
id	String	Specifies the ID of the backend server group.
tenant_id	String	Specifies the ID of the project where the backend server group is used. The value contains a maximum of 255 characters.
project_id	String	Specifies the ID of the project to which the backend server group belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the name of the backend server group. The value contains a maximum of 255 characters.

Parameter	Type	Description
description	String	Provides supplementary information about the backend server group. The value contains a maximum of 255 characters.
protocol	String	Specifies the protocol that the backend server group uses to receive requests. TCP, UDP, and HTTP are supported. When a backend server group is associated with a listener, the relationships between the protocol used by the listener and the protocol of the backend server group are as follows: • When the protocol used by the listener is **UDP**, the protocol of the backend server group must be **UDP**. • When the protocol used by the listener is **TCP**, the protocol of the backend server group must be **TCP**. • When the protocol used by the listener is **HTTP** or **TERMINATED_HTTPS**, the protocol of the backend server group must be **HTTP**.
lb_algorithm	String	Specifies the load balancing algorithm of the backend server group. The value range varies depending on the protocol of the backend server group: • **ROUND_ROBIN**: indicates the weighted round robin algorithm. • **LEAST_CONNECTIONS**: indicates the weighted least connections algorithm. • **SOURCE_IP**: indicates the source IP hash algorithm. When the value is **SOURCE_IP**, the weights of backend servers in the server group are invalid.
members	Array of **Members** objects	Lists the IDs of backend servers in the backend server group. For details, see **Table 6-79**.
healthmonitor_id	String	Specifies the ID of the health check configured for the backend server group.

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the backend server group. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
listeners	Array of **Listeners** objects	Lists the IDs of listeners associated with the backend server group. For details, see **Table 6-80**.
loadbalancers	Array of **Loadbalancers** objects	Lists the IDs of load balancers associated with the backend server group. For details, see **Table 6-81**.
session_persistence	**SessionPersistence** object	Specifies whether to enable the sticky session feature. For details, see **Table 6-82**. Once sticky session are enabled, requests from the same client are sent to the same backend server during the session. When sticky sessions are disabled, the value is **null**.
protection_status	String	String Specifies whether modification protection is enabled. The value can be one of the following: • **nonProtection** (default): Modification protection is not enabled. • **consoleProtection**: Modification protection is enabled to avoid that resources are modified by accident on the console.
protection_reason	String	String Specifies the reason to enable modification protection. This parameter is valid only when **protection_status** is set to **consoleProtection**.

Table 6-104 members parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated backend server.

Table 6-105 listeners parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated backend server group.

Table 6-106 loadbalancers parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated load balancer.

Table 6-107 session_persistence parameter description

Parameter	Mandatory	Type	Description
type	Yes	String	Specifies the sticky session type. The value can be: • **SOURCE_IP**: Requests are distributed based on the client's IP address. Requests from the same IP address are sent to the same backend server. • **HTTP_COOKIE**: When the client sends a request for the first time, the load balancer automatically generates a cookie and inserts the cookie into the response message. Subsequent requests are sent to the backend server that processes the first request. • **APP_COOKIE**: When the client sends a request for the first time, the backend server that receives the request generates a cookie and inserts the cookie into the response message. Subsequent requests are sent to this backend server. When the protocol of the backend server group is TCP, only **SOURCE_IP** takes effect. When the protocol of the backend server group is HTTP, only **HTTP_COOKIE** or **APP_COOKIE** takes effect.

Parameter	Mandatory	Type	Description
cookie_name	No	String	Specifies the cookie name. The name can contain up to 64 characters, including letters, digits, hyphens (-), and underscores (_). This parameter is mandatory when the sticky session type is **APP_COOKIE**.
persistence_timeout	No	Integer	Specifies the sticky session timeout duration in minutes. This parameter is invalid when **type** is set to **APP_COOKIE**. The value range varies depending on the protocol of the backend server group: • When the protocol of the backend server group is TCP or UDP, the value ranges from **1** to **60**. • When the protocol of the backend server group is HTTP or HTTPS, the value ranges from **1** to **1440**.

Example Request

- Example request: Updating the name, description, and load balancing algorithm of a backend server group

```
PUT https://{Endpoint}/v2/1a3e005cf9ce40308c900bcb08e5320c/elb/pools/12ff63af-4127-4074-a251-bcb2ecc53ebe

{
    "pool": {
        "name": "pool2",
        "description": "pool two",
        "lb_algorithm": "LEAST_CONNECTIONS"
    }
}
```

Example Response

- Example response 1

```
{
    "pool": {
        "lb_algorithm": "LEAST_CONNECTIONS",
        "protocol": "HTTP",
        "description": "pool two",
        "admin_state_up": false,
        "tenant_id": "1a3e005cf9ce40308c900bcb08e5320c",
        "project_id": "1a3e005cf9ce40308c900bcb08e5320c",
        "session_persistence": {
            "cookie_name": null,
            "type": "HTTP_COOKIE",
            "persistence_timeout": 1440
        },
```



```
    "healthmonitor_id": null,
    "listeners": [
      {
        "id": "39de4d56-d663-46e5-85a1-5b9d5fa17829"
      }
    ],
    "members": [],
    "id": "12ff63af-4127-4074-a251-bcb2ecc53ebe",
    "name": "pool2"
  }
}
```


Status Code

For details, see **Status Codes**.

6.3.5 Deleting a Backend Server Group

Function

This API is used to delete a backend server group.

Constraints

Before deleting a backend server group, remove all backend servers, delete the health check, and disassociate forwarding policies from the backend server group by changing the value of **redirect_pool_id** to **null**. For details, see **Updating a Forwarding Policy**.

URI

DELETE /v2/{project_id}/elb/pools/{pool_id}

Table 6-108 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
pool_id	Yes	String	Specifies the ID of the backend server group.

Request

None

Response

None

Example Request

- Example request: Deleting a backend server group
  DELETE https://{Endpoint}/v2/1a3e005cf9ce40308c900bcb08e5320c/elb/pools/5a9a3e9e-d1aa-448e-af37-a70171f2a332

Example Response

- Example response

  None

Status Code

For details, see **Status Codes**.

6.4 Backend Server

6.4.1 Adding a Backend Server

Function

This API is used to add a backend server to a specific backend server group. After a backend server group is added to a listener, traffic is distributed to backend servers in this server group using the specified load balancing algorithm.

Constraints

Two backend servers in a backend server group cannot have the same private IP address or port number.

The subnet specified during server creation must be in the same VPC as the subnet from which the private IP address of the load balancer is assigned.

You can call this API for a maximum of 200 times per minute globally.

URI

POST /v2/{project_id}/elb/pools/{pool_id}/members

Table 6-109 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
pool_id	Yes	String	Specifies the ID of the backend server group.

Request

Table 6-110 Parameter description

Parameter	Mandatory	Type	Description
member	Yes	**Member** object	Specifies the backend server. For details, see **Table 6-111**.

Table 6-111 member parameter description

Parameter	Mandatory	Type	Description
tenant_id	No	String	Specifies the ID of the project where the backend server is used. The value must be the same as the value of **project_id** in the token. The value contains a maximum of 255 characters.
name	No	String	Specifies the backend server name. The value is an empty character string by default. The value contains a maximum of 255 characters.
address	Yes	String	Specifies the private IP address of the backend server. This IP address must be in the subnet specified by **subnet_id**. This parameter can be set only to the IP address of the primary NIC, for example, 192.168.3.11. The value contains a maximum of 64 characters.
protocol_port	Yes	Integer	Specifies the port used by the backend server. The port number ranges from 1 to 65535.
subnet_id	Yes	String	Specifies the ID of the subnet where the backend server resides. The private IP address of the backend server is in this subnet. Only IPv4 subnets are supported.

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Specifies the administrative status of the backend server. This parameter is reserved, and the default value is **true**.
weight	No	Integer	Specifies the backend server weight. The value ranges from **0** to **100**. If the value is **0**, the backend server will not accept new requests. The default value is **1**.

Response

Table 6-112 Parameter description

Parameter	Type	Description
member	**Member** object	Specifies the backend server. For details, see **Table 6-113**.

Table 6-113 member parameter description

Parameter	Type	Description
id	String	Specifies the backend server ID. **NOTE** The value of this parameter is not the ID of server. It is the ID automatically generated for the backend server associated with the load balancer.
tenant_id	String	Specifies the ID of the project where the backend server is used. The value contains a maximum of 255 characters.
project_id	String	Specifies the ID of the project to which the backend server belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the backend server name. The value contains a maximum of 255 characters.

Parameter	Type	Description
address	String	Specifies the private IP address of the backend server. This IP address must be in the subnet specified by **subnet_id**. This parameter can be set only to the IP address of the primary NIC, for example, 192.168.3.11. The value contains a maximum of 64 characters.
protocol_port	Integer	Specifies the port used by the backend server. The port number ranges from 1 to 65535.
subnet_id	String	Specifies the ID of the subnet where the backend server resides. The private IP address of the backend server is in this subnet. IPv6 subnets are not supported.
admin_state_up	Boolean	Specifies the administrative status of the backend server. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
weight	Integer	Specifies the backend server weight. The value ranges from **0** to **100**. If the value is **0**, the backend server will not accept new requests. The default value is **1**.
operating_status	String	Specifies the health check result of the backend server. The value can be one of the following: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group that the backend server belongs to. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist.

Example Request

- Adding a backend server

  Obtain the values of **subnet_id** and **ip_address** by querying the subnet ID and IP address of the server associated with the load balancer.

  Alternatively, query the subnet ID and IP address using the server ID. **device_id** in the request indicates the server ID. Obtain the values of **subnet_id** and **ip_address** of the primary NIC (the port for which **primary_interface** is **true**) in the response body.

```
POST https://{Endpoint}/v2/145483a5107745e9b3d80f956713e6a3/elb/pools/5a9a3e9e-d1aa-448e-af37-a70171f2a332/members

{
    "member": {
        "subnet_id": "33d8b01a-bbe6-41f4-bc45-78a1d284d503",
        "protocol_port": 88,
        "name": "member-jy-tt-1",
        "address": "192.168.44.11"
    }
}
```

Example Response

- Example response

```
{
    "member": {
        "name": "member-jy-tt-1",
        "weight": 1,
        "admin_state_up": true,
        "subnet_id": "33d8b01a-bbe6-41f4-bc45-78a1d284d503",
        "tenant_id": "145483a5107745e9b3d80f956713e6a3",
        "project_id": "145483a5107745e9b3d80f956713e6a3",
        "address": "192.168.44.11",
        "protocol_port": 88,
        "operating_status": "ONLINE",
        "id": "c0042496-e220-44f6-914b-e6ca33bab503"
    }
}
```

Status Code

For details, see **Status Codes**.

6.4.2 Querying Backend Servers

Function

This API is used to query backend servers in a specific backend server group. Filter query and pagination query are supported. Unless otherwise specified, exact match is applied.

URI

GET /v2/{project_id}/elb/pools/{pool_id}/members

Table 6-114 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
pool_id	Yes	String	Specifies the ID of the backend server group.

Table 6-115 Query parameters

Parameter	Mandatory	Type	Description
marker	No	String	Specifies the ID of the backend server from which pagination query starts, that is, the ID of the last backend server on the previous page. If this parameter is not specified, the first page will be queried. This parameter must be used together with **limit**.
limit	No	Integer	Specifies the number of backend servers on each page. If this parameter is not set, all backend servers are queried by default.
page_reverse	No	Boolean	Specifies the page direction. The value can be **true** or **false**, and the default value is **false**. The last page in the list requested with **page_reverse** set to **false** will not contain the "next" link, and the last page in the list requested with **page_reverse** set to **true** will not contain the "previous" link. This parameter must be used together with **limit**.
id	No	String	Specifies the backend server ID. **NOTE** The value of this parameter is not the ID of server. It is the ID automatically generated for the backend server associated with the load balancer.

Parameter	Mandatory	Type	Description
tenant_id	No	String	Specifies the ID of the project where the backend server is used. The value contains a maximum of 255 characters.
project_id	No	String	Specifies the ID of the project to which the backend server belongs. This parameter has the same meaning as **tenant_id**.
name	No	String	Specifies the backend server name. The value contains a maximum of 255 characters. **NOTE** The value of this parameter is not the name of server. It is the name automatically generated for the backend server associated with the load balancer.
address	No	String	Specifies the private IP address of the backend server. The value contains a maximum of 64 characters.
protocol_port	No	Integer	Specifies the port used by the backend server.
subnet_id	No	String	Specifies the ID of the subnet where the backend server resides.
admin_state_up	No	Boolean	Specifies the administrative status of the backend server. This parameter is reserved, and the default value is **true**.
weight	No	Integer	Specifies the backend server weight.

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Specifies the enterprise project ID. • If **enterprise_project_id** is not passed, resources in all enterprise projects are queried by default. Fine-grained authorization is performed. The **elb:*list** permissions must be assigned to the user group. • If **enterprise_project_id** is passed, the value can be a specific enterprise project ID or **all_granted_eps**. If the value is a specific enterprise project ID, only resources in the enterprise project are queried. If the value is **all_granted_eps**, resources in the enterprise projects with the **elb:*list** permissions are queried.

Request

None

Response

Table 6-116 Parameter description

Parameter	Type	Description
members	Array of **Members** objects	Lists backend servers in the backend server group. For details, see **Table 6-117**.

Table 6-117 members parameter description

Parameter	Type	Description
id	String	Specifies the backend server ID. **NOTE** The value of this parameter is not the ID of server. It is the ID automatically generated for the backend server associated with the load balancer.

Parameter	Type	Description
tenant_id	String	Specifies the ID of the project where the backend server is used. The value contains a maximum of 255 characters.
project_id	String	Specifies the ID of the project to which the backend server belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the backend server name. The value contains a maximum of 255 characters.
address	String	Specifies the private IP address of the backend server. This IP address must be in the subnet specified by **subnet_id**. This parameter can be set only to the IP address of the primary NIC, for example, 192.168.3.11. The value contains a maximum of 64 characters.
protocol_port	Integer	Specifies the port used by the backend server. The port number ranges from 1 to 65535.
subnet_id	String	Specifies the ID of the subnet where the backend server resides. The private IP address of the backend server is in this subnet. IPv6 subnets are not supported.
admin_state_up	Boolean	Specifies the administrative status of the backend server. This parameter is reserved. The value can be **true** or **false**. ● **true**: Enabled ● **false**: Disabled
weight	Integer	Specifies the backend server weight. The value ranges from **0** to **100**. If the value is **0**, the backend server will not accept new requests. The default value is **1**.

Parameter	Type	Description
operating_status	String	Specifies the health check result of the backend server. The value can be one of the following: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group that the backend server belongs to. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist.

Example Request

- Example request 1: Querying all backend servers
  ```
  GET https://{Endpoint}/v2/1a3e005cf9ce40308c900bcb08e5320c/elb/pools/5a9a3e9e-d1aa-448e-af37-a70171f2a332/members
  ```
- Example request 2: Querying the backend cloud server whose IP address is 10.0.0.8 and port number is 80
  ```
  GET https://{Endpoint}/v2/1a3e005cf9ce40308c900bcb08e5320c/elb/pools/5a9a3e9e-d1aa-448e-af37-a70171f2a332/members?address=10.0.0.8&protocol_port=80
  ```

Example Response

- Example response 1
  ```
  {
     "members": [
        {
           "address": "10.0.0.8",
           "admin_state_up": true,
           "id": "9a7aff27-fd41-4ec1-ba4c-3eb92c629313",
           "protocol_port": 80,
           "subnet_id": "013d3059-87a4-45a5-91e9-d721068ae0b2",
           "tenant_id": "1a3e005cf9ce40308c900bcb08e5320c",
           "project_id": "1a3e005cf9ce40308c900bcb08e5320c",
           "weight": 1,
           "operating_status": "ONLINE",
           "name": "member-name"
        }
     ]
  }
  ```
- Example response 2
  ```
  {
     "members": [
        {
           "address": "10.0.0.8",
           "admin_state_up": true,
           "id": "9a7aff27-fd41-4ec1-ba4c-3eb92c629313",
           "protocol_port": 80,
           "subnet_id": "013d3059-87a4-45a5-91e9-d721068ae0b2",
           "tenant_id": "1a3e005cf9ce40308c900bcb08e5320c",
           "project_id": "1a3e005cf9ce40308c900bcb08e5320c",
           "weight": 1,
           "operating_status": "ONLINE",
           "name": "member-name"
        }
     ]
  }
  ```


Status Code

For details, see **Status Codes**.

6.4.3 Querying Details of a Backend Server

Function

This API is used to query details of a backend server.

URI

GET /v2/{project_id}/elb/pools/{pool_id}/members/{member_id}

Table 6-118 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
pool_id	Yes	String	Specifies the ID of the backend server group.
member_id	Yes	String	Specifies the backend server ID. **NOTE** • The value of this parameter is not the ID of the server. It is an ID automatically generated for the backend server that is associated with the load balancer. • You can obtain this value by calling the API described in **Querying Backend Servers**.

Request

None

Response

Table 6-119 Parameter description

Parameter	Type	Description
member	**Member** object	Specifies the backend server. For details, see **Table 6-120**.

Table 6-120 member parameter description

Parameter	Type	Description
id	String	Specifies the backend server ID. **NOTE** The value of this parameter is not the ID of server. It is the ID automatically generated for the backend server associated with the load balancer.
tenant_id	String	Specifies the ID of the project where the backend server is used. The value contains a maximum of 255 characters.
project_id	String	Specifies the ID of the project to which the backend server belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the backend server name. The value contains a maximum of 255 characters.
address	String	Specifies the private IP address of the backend server. This IP address must be in the subnet specified by **subnet_id**. This parameter can be set only to the IP address of the primary NIC, for example, 192.168.3.11. The value contains a maximum of 64 characters.
protocol_port	Integer	Specifies the port used by the backend server. The port number ranges from 1 to 65535.
subnet_id	String	Specifies the ID of the subnet where the backend server resides. The private IP address of the backend server is in this subnet. IPv6 subnets are not supported.
admin_state_up	Boolean	Specifies the administrative status of the backend server. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled

Parameter	Type	Description
weight	Integer	Specifies the backend server weight. The value ranges from **0** to **100**. If the value is **0**, the backend server will not accept new requests. The default value is **1**.
operating_status	String	Specifies the health check result of the backend server. The value can be one of the following: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group that the backend server belongs to. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist.

Example Request

- Example request: Querying details of a backend server
  ```
  GET https://{Endpoint}/v2/145483a5107745e9b3d80f956713e6a3/elb/pools/5a9a3e9e-d1aa-448e-af37-a70171f2a332/members/cf024846-7516-4e3a-b0fb-6590322c836f
  ```
  Example request 2: Querying the EIP bound to a load balancer
- For details, see **Querying EIPs**.
- Example request
  ```
  GET https://{EIP_Endpoint}/v1/{project_id}/publicips?port_id={vip_port_id}
  ```
  vip_port_id is the value of **vip_port_id** of the load balancer.

Example Response

- Example response 1
  ```
  {
     "member": {
        "name": "",
        "weight": 1,
        "admin_state_up": true,
        "subnet_id": "823d5866-6e30-45c2-9b1a-a1ebc3757fdb",
        "tenant_id": "145483a5107745e9b3d80f956713e6a3",
        "project_id": "145483a5107745e9b3d80f956713e6a3",
        "address": "192.172.3.100",
        "protocol_port": 8080,
        "operating_status": "ONLINE",
        "id": "e58f5bfa-0e46-4bc5-951c-8473d3e5f24a"
     }
  }
  ```
- Example response 2
  ```
  {
     "publicips": [
        {
           "id": "6285e7be-fd9f-497c-bc2d-dd0bdea6efe0",
  ```



```
        "status": "DOWN",
        "profile": {
          "user_id": "35f2b308f5d64441a6fa7999fbcd4321",
          "product_id": "00301-48027-0--0",
          "region_id": "xxx",
          "order_id": "xxxxxxxxx"
        },
        "type": "5_bgp",
        "public_ip_address": "161.xx.xx.9",
        "private_ip_address": "192.168.2.4",
        "tenant_id": "8b7e35ad379141fc9df3e178bd64f55c",
        "create_time": "2015-07-16 04:22:32",
        "bandwidth_id": "3fa5b383-5a73-4dcb-a314-c6128546d855",
        "bandwidth_share_type": "PER",
        "bandwidth_size": 5,
        "bandwidth_name": "bandwidth-test",
        "enterprise_project_id":"b261ac1f-2489-4bc7-b31b-c33c3346a439",
        "ip_version": 4,
        "port_id": "c7157e7a-036a-42ca-8474-100be22e3727"
    }
  ]
}
```


public_ip_address indicates the EIP bound to the load balancer.

Status Code

For details, see **Status Codes**.

6.4.4 Updating a Backend Server

Function

This API is used to update a backend server. You can modify its name and weight. You can set a larger weight for backend servers that can receive more traffic.

Constraints

If the provisioning status of the associated load balancer is not **ACTIVE**, the backend server cannot be updated.

URI

PUT /v2/{project_id}/elb/pools/{pool_id}/members/{member_id}

Table 6-121 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
pool_id	Yes	String	Specifies the ID of the backend server group.

Parameter	Mandatory	Type	Description
member_id	Yes	String	Specifies the backend server ID. **NOTE** • The value of this parameter is not the ID of the server. It is an ID automatically generated for the backend server that is associated with the load balancer. • You can obtain this value by calling the API described in **Querying Backend Servers**.

Request

Table 6-122 Parameter description

Parameter	Mandatory	Type	Description
member	Yes	**Member** object	Specifies the backend server. For details, see **Table 6-123**.

Table 6-123 member parameter description

Parameter	Mandatory	Type	Description
name	No	String	Specifies the backend server name. The value contains a maximum of 255 characters.
admin_state_up	No	Boolean	Specifies the administrative status of the backend server. This parameter is reserved, and the default value is **true**.
weight	No	Integer	Specifies the backend server weight. The value ranges from **0** to **100**. If the value is **0**, the backend server will not accept new requests. The default value is **1**.

Response

Table 6-124 Parameter description

Parameter	Type	Description
member	**Member** object	Specifies the backend server. For details, see **Table 6-125**.

Table 6-125 member parameter description

Parameter	Type	Description
id	String	Specifies the backend server ID. **NOTE** The value of this parameter is not the ID of server. It is the ID automatically generated for the backend server associated with the load balancer.
tenant_id	String	Specifies the ID of the project where the backend server is used. The value contains a maximum of 255 characters.
project_id	String	Specifies the ID of the project to which the backend server belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the backend server name. The value contains a maximum of 255 characters.
address	String	Specifies the private IP address of the backend server. This IP address must be in the subnet specified by **subnet_id**. This parameter can be set only to the IP address of the primary NIC, for example, 192.168.3.11. The value contains a maximum of 64 characters.
protocol_port	Integer	Specifies the port used by the backend server. The port number ranges from 1 to 65535.
subnet_id	String	Specifies the ID of the subnet where the backend server resides. The private IP address of the backend server is in this subnet. IPv6 subnets are not supported.

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the backend server. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
weight	Integer	Specifies the backend server weight. The value ranges from **0** to **100**. If the value is **0**, the backend server will not accept new requests. The default value is **1**.
operating_status	String	Specifies the health check result of the backend server. The value can be one of the following: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group that the backend server belongs to. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist.

Example Request

- Example request: Updating the name and weight of a backend server

```
PUT https://{Endpoint}/v2/145483a5107745e9b3d80f956713e6a3/elb/pools/5a9a3e9e-d1aa-448e-af37-a70171f2a332/members/c0042496-e220-44f6-914b-e6ca33bab503

{
    "member": {
        "name": "member create test",
        "weight": 10
    }
}
```

Example Response

- Example response

```
{
    "member": {
        "name": "member-jy-tt-1",
        "weight": 1,
        "admin_state_up": true,
        "subnet_id": "33d8b01a-bbe6-41f4-bc45-78a1d284d503",
        "tenant_id": "145483a5107745e9b3d80f956713e6a3",
        "project_id": "145483a5107745e9b3d80f956713e6a3",
        "address": "192.168.44.11",
        "protocol_port": 88,
        "operating_status": "ONLINE",
```



```
        "id": "c0042496-e220-44f6-914b-e6ca33bab503"
    }
}
```

Status Code

For details, see **Status Codes**.

6.4.5 Removing a Backend Server

Function

This API is used to remove a backend server by its ID.

Constraints

After you remove a backend server, new connections to this server will not be established. However, long connections that have been established will be maintained.

URI

DELETE /v2/{project_id}/elb/pools/{pool_id}/members/{member_id}

Table 6-126 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
pool_id	Yes	String	Specifies the ID of the backend server group.
member_id	Yes	String	Specifies the backend server ID. **NOTE** • The value of this parameter is not the ID of the server. It is an ID automatically generated for the backend server that is associated with the load balancer. • You can obtain this value by calling the API described in **Querying Backend Servers**.

Request

None

Response

None

Example Request

- Example request: Removing a backend server
  DELETE https://{Endpoint}/v2/145483a5107745e9b3d80f956713e6a3/elb/pools/5a9a3e9e-d1aa-448e-af37-a70171f2a332/members/cf024846-7516-4e3a-b0fb-6590322c836f

Example Response

- Example response

  None

Status Code

For details, see **Status Codes**.

6.5 Health Check

6.5.1 Configuring a Health Check

Function

This API is used to configure a health check for a backend server group to check the status of backend servers. If the health check result is **OFFLINE**, backend servers are considered unhealthy. You need to check the server configuration.

Constraints

- The security groups must have rules that allow access by 100.125.0.0/16.
- If UDP is used for the health check, the protocol of the backend server group must be UDP.

URI

POST /v2/{project_id}/elb/healthmonitors

Table 6-127 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Request

Table 6-128 Parameter description

Parameter	Mandatory	Type	Description
healthmonitor	Yes	**Healthmonitor** object	Specifies the health check. For details, see **Table 6-129**.

Table 6-129 healthmonitor parameter description

Parameter	Mandatory	Type	Description
tenant_id	No	String	Specifies the ID of the project where the health check is performed. The value must be the same as the value of **project_id** in the token. The value contains a maximum of 255 characters.
name	No	String	Specifies the health check name. The value contains a maximum of 255 characters.
delay	Yes	Integer	Specifies the maximum time between health checks in the unit of second. The value ranges from **1** to **50**.
max_retries	Yes	Integer	Specifies the maximum number of retries. The value ranges from **1** to **10**.
pool_id	Yes	String	Specifies the ID of the backend server group. Only one health check can be configured for each backend server group.
admin_state_up	No	Boolean	Specifies the administrative status of the health check. This parameter is reserved, and the default value is **true**.

Parameter	Mandatory	Type	Description
timeout	Yes	Integer	Specifies the health check timeout duration in the unit of second. The value ranges from **1** to **50**. **NOTE** You are advised to set the value less than that of parameter **delay**.
type	Yes	String	Specifies the health check protocol. The value can be **TCP**, **UDP_CONNECT**, or **HTTP**.
monitor_port	No	Integer	Specifies the health check port. The port number ranges from 1 to 65535. The value is left blank by default, indicating that the port of the backend server is used as the health check port.
domain_name	No	String	Specifies the domain name of HTTP requests during the health check. This parameter takes effect only when the value of **type** is set to **HTTP**. The value is left blank by default, indicating that the private IP address of the load balancer is used as the destination address of HTTP requests. The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter, for example, www.test.com. The value contains a maximum of 100 characters.

Parameter	Mandatory	Type	Description
url_path	No	String	Specifies the HTTP request path for the health check. The default value is **/**. The value starts with a slash (/). This parameter takes effect only when the value of **type** is set to **HTTP**. An example value is **/test**. The value contains a maximum of 80 characters.
expected_codes	No	String	Specifies the expected HTTP status code. The following options are available: A single value, such as **200** A list of values, such as **200,202** A value range, such as **200–204** This parameter takes effect only when the value of **type** is set to **HTTP**. The value contains a maximum of 64 characters. **NOTE** This parameter is reserved.
http_method	No	String	Specifies the HTTP request method. The default value is **GET**. The value can be **GET**, **HEAD**, **POST**, **PUT**, **DELETE**, **TRACE**, **OPTIONS**, **CONNECT**, or **PATCH**. This parameter takes effect only when the value of **type** is set to **HTTP**. **NOTE** This parameter is reserved.

Response

Table 6-130 Parameter description

Parameter	Type	Description
healthmonitor	**Healthmonitor** object	Specifies the health check. For details, see **Table 6-131**.

Table 6-131 healthmonitor parameter description

Parameter	Type	Description
id	String	Specifies the health check ID.
tenant_id	String	Specifies the ID of the project where the health check is performed.
project_id	String	Specifies the ID of the project to which the health check belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the health check name.
delay	Integer	Specifies the maximum time between health checks in the unit of second. The value ranges from **1** to **50**.
max_retries	Integer	Specifies the maximum number of retries. The value ranges from **1** to **10**.
max_retries_down	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **ONLINE** to **OFFLINE**. The value ranges from **1** to **10**.
pools	Array of **Pools** objects	Lists the IDs of backend server groups associated with the health check. For details, see **Table 6-132**.
admin_state_up	Boolean	Specifies the administrative status of the health check. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
timeout	Integer	Specifies the health check timeout duration in the unit of second. The value ranges from **1** to **50**. **NOTE** You are advised to set the value less than that of parameter **delay**.

Parameter	Type	Description
type	String	Specifies the health check protocol. The value can be **TCP**, **UDP_CONNECT**, or **HTTP**.
monitor_port	Integer	Specifies the health check port. The port number ranges from 1 to 65535. The value is left blank by default, indicating that the port of the backend server is used as the health check port.
expected_codes	String	Specifies the expected HTTP status code. The following options are available: A single value, such as **200** A list of values, such as **200,202** A value range, such as **200–204** This parameter takes effect only when the value of **type** is set to **HTTP**. Currently, this parameter is not supported and is fixed at **200**.
domain_name	String	Specifies the domain name of HTTP requests during the health check. This parameter takes effect only when the value of **type** is set to **HTTP**. The value is left blank by default, indicating that the private IP address of the load balancer is used as the destination address of HTTP requests. The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter, for example: www.test.com.
url_path	String	Specifies the HTTP request path for the health check. The default value is **/**. The value starts with a slash (/). This parameter takes effect only when the value of **type** is set to **HTTP**. An example value is **/test**.

Parameter	Type	Description
http_method	String	Specifies the HTTP request method. The default value is **GET**. The value can be **GET**, **HEAD**, **POST**, **PUT**, **DELETE**, **TRACE**, **OPTIONS**, **CONNECT**, or **PATCH**. This parameter takes effect only when the value of **type** is set to **HTTP**. **NOTE** This parameter is reserved.

Table 6-132 pools parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	Specifies the ID of the backend server group.

Example Request

- Example request: Configuring a health check

```
POST https://{Endpoint}/v2/145483a5107745e9b3d80f956713e6a3/elb/healthmonitors

{
  "healthmonitor": {
    "admin_state_up": true,
    "pool_id": "bb44bffb-05d9-412c-9d9c-b189d9e14193",
    "domain_name": "www.test.com",
    "delay": 10,
    "max_retries": 10,
    "timeout": 10,
    "type": "HTTP"
  }
}
```

Example Response

- Example response 1

```
{
  "healthmonitor": {
    "name": "",
    "admin_state_up": true,
    "tenant_id": "145483a5107745e9b3d80f956713e6a3",
    "project_id": "145483a5107745e9b3d80f956713e6a3",
    "domain_name": "www.test.com",
    "delay": 10,
    "expected_codes": "200",
    "max_retries": 10,
    "http_method": "GET",
    "timeout": 10,
    "pools": [
      {
        "id": "bb44bffb-05d9-412c-9d9c-b189d9e14193"
      }
    ],
```



```
    "url_path": "/",
    "type": "HTTP",
    "id": "2dca3867-98c5-4cde-8f2c-b89ae6bd7e36",
    "monitor_port": 112
  }
}
```

Status Code

For details, see **Status Codes**.

6.5.2 Querying Health Checks

Function

This API is used to query all the health checks. Filter query and pagination query are supported. Unless otherwise specified, exact match is applied.

URI

GET /v2/{project_id}/elb/healthmonitors

Table 6-133 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Table 6-134 Query parameters

Parameter	Mandatory	Type	Description
marker	No	String	Specifies the ID of the health check from which pagination query starts, that is, the ID of the last health check on the previous page. This parameter must be used together with **limit**.
limit	No	Integer	Specifies the number of health checks on each page. If this parameter is not set, all health checks are queried by default.

Parameter	Mandatory	Type	Description
page_reverse	No	Boolean	Specifies the page direction. The value can be **true** or **false**, and the default value is **false**. The last page in the list requested with **page_reverse** set to **false** will not contain the "next" link, and the last page in the list requested with **page_reverse** set to **true** will not contain the "previous" link. This parameter must be used together with **limit**.
id	No	String	Specifies the health check ID.
tenant_id	No	String	Specifies the ID of the project where the health check is performed. The value contains a maximum of 255 characters.
project_id	No	String	Specifies the ID of the project to which the health check belongs. This parameter has the same meaning as **tenant_id**.
name	No	String	Specifies the health check name. The value contains a maximum of 255 characters.
delay	No	Integer	Specifies the maximum time between health checks in the unit of second. The value ranges from **1** to **50**.
max_retries	No	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **OFFLINE** to **ONLINE**. The value ranges from **1** to **10**.
admin_state_up	No	Boolean	Specifies the administrative status of the health check. The value can be **true** or **false**. The default value is **true**. • **true**: indicates that the health check function is enabled. • **false**: indicates that the health check function is disabled.

Parameter	Mandatory	Type	Description
timeout	No	Integer	Specifies the health check timeout duration in the unit of second. The value ranges from **1** to **50**. **NOTE** You are advised to set the value less than that of parameter **delay**.
type	No	String	Specifies the health check protocol. The value can be **TCP**, **UDP_CONNECT**, or **HTTP**.
monitor_port	No	Integer	Specifies the port used for the health check. The value is left blank by default, indicating that the port of the backend server is used as the health check port.
expected_codes	No	String	Specifies the expected HTTP status code. The following options are available: A single value, such as **200** A list of values, such as **200,202** A value range, such as **200–204** This parameter takes effect only when the value of **type** is set to **HTTP**. The value contains a maximum of 64 characters. **NOTE** This parameter is reserved.
domain_name	No	String	Specifies the domain name of HTTP requests during the health check. This parameter takes effect only when the value of **type** is set to **HTTP**. The value is left blank by default, indicating that the private IP address of the load balancer is used as the destination address of HTTP requests. The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter, for example: www.test.com. The value contains a maximum of 100 characters.

Parameter	Mandatory	Type	Description
url_path	No	String	Specifies the HTTP request path for the health check. The default value is **/**. The value starts with a slash (/). This parameter takes effect only when the value of **type** is set to **HTTP**. An example value is **/test**. The value contains a maximum of 80 characters.
http_method	No	String	Specifies the HTTP request method. The default value is **GET**. The value can be **GET**, **HEAD**, **POST**, **PUT**, **DELETE**, **TRACE**, **OPTIONS**, **CONNECT**, or **PATCH**. This parameter takes effect only when the value of **type** is set to **HTTP**. **NOTE** This parameter is reserved.

Request

None

Response

Table 6-135 Parameter description

Parameter	Type	Description
healthmonitors	Array of **Healthmonitors** objects	Lists the health checks. For details, see **Table 6-136**.

Table 6-136 healthmonitor parameter description

Parameter	Type	Description
id	String	Specifies the health check ID.
tenant_id	String	Specifies the ID of the project where the health check is performed.
project_id	String	Specifies the ID of the project to which the health check belongs. This parameter has the same meaning as **tenant_id**.

Parameter	Type	Description
name	String	Specifies the health check name.
delay	Integer	Specifies the maximum time between health checks in the unit of second. The value ranges from **1** to **50**.
max_retries	Integer	Specifies the maximum number of retries. The value ranges from **1** to **10**.
max_retries_down	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **ONLINE** to **OFFLINE**. The value ranges from **1** to **10**.
pools	Array of **Pools** objects	Lists the IDs of backend server groups associated with the health check. For details, see **Table 6-132**.
admin_state_up	Boolean	Specifies the administrative status of the health check. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
timeout	Integer	Specifies the health check timeout duration in the unit of second. The value ranges from **1** to **50**. **NOTE** You are advised to set the value less than that of parameter **delay**.
type	String	Specifies the health check protocol. The value can be **TCP**, **UDP_CONNECT**, or **HTTP**.
monitor_port	Integer	Specifies the health check port. The port number ranges from 1 to 65535. The value is left blank by default, indicating that the port of the backend server is used as the health check port.

Parameter	Type	Description
expected_codes	String	Specifies the expected HTTP status code. The following options are available: A single value, such as **200** A list of values, such as **200,202** A value range, such as **200–204** This parameter takes effect only when the value of **type** is set to **HTTP**. Currently, this parameter is not supported and is fixed at **200**.
domain_name	String	Specifies the domain name of HTTP requests during the health check. This parameter takes effect only when the value of **type** is set to **HTTP**. The value is left blank by default, indicating that the private IP address of the load balancer is used as the destination address of HTTP requests. The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter, for example: www.test.com.
url_path	String	Specifies the HTTP request path for the health check. The default value is **/**. The value starts with a slash (/). This parameter takes effect only when the value of **type** is set to **HTTP**. An example value is **/test**.
http_method	String	Specifies the HTTP request method. The default value is **GET**. The value can be **GET**, **HEAD**, **POST**, **PUT**, **DELETE**, **TRACE**, **OPTIONS**, **CONNECT**, or **PATCH**. This parameter takes effect only when the value of **type** is set to **HTTP**. **NOTE** This parameter is reserved.

Table 6-137 pools parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	Specifies the ID of the backend server group.

Example Request

- Example request 1: Querying all health checks
  GET https://{Endpoint}/v2/601240b9c5c94059b63d484c92cfe308/elb/healthmonitors
- Example request 2: Querying HTTP health checks
  GET https://{Endpoint}/v2/601240b9c5c94059b63d484c92cfe308/elb/healthmonitors?type=HTTP

Example Response

- Example response 1

```
{
   "healthmonitors": [
      {
         "monitor_port": null,
         "name": "",
         "admin_state_up": true,
         "tenant_id": "601240b9c5c94059b63d484c92cfe308",
         "project_id": "601240b9c5c94059b63d484c92cfe308",
         "domain_name": null,
         "delay": 5,
         "expected_codes": "200",
         "max_retries": 3,
         "http_method": "GET",
         "timeout": 10,
         "pools": [
            {
               "id": "caef8316-6b65-4676-8293-cf41fb63cc2a"
            }
         ],
         "url_path": "/",
         "type": "HTTP",
         "id": "1b587819-d619-49c1-9101-fe72d8b361ef"
      }
   ]
}
```

- Example response 2

```
{
   "healthmonitors": [
      {
         "monitor_port": null,
         "name": "",
         "admin_state_up": true,
         "tenant_id": "601240b9c5c94059b63d484c92cfe308",
         "project_id": "601240b9c5c94059b63d484c92cfe308",
         "domain_name": null,
         "delay": 5,
         "expected_codes": "200",
         "max_retries": 3,
         "http_method": "GET",
         "timeout": 10,
         "pools": [
            {
               "id": "caef8316-6b65-4676-8293-cf41fb63cc2a"
            }
         ],
         "url_path": "/",
         "type": "HTTP",
         "id": "1b587819-d619-49c1-9101-fe72d8b361ef"
      }
   ]
}
```


Status Code

For details, see **Status Codes**.

6.5.3 Querying Health Check Details

Function

This API is used to query details about a health check.

URI

GET /v2/{project_id}/elb/healthmonitors/{healthmonitor_id}

Table 6-138 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
healthmonitor_id	Yes	String	Specifies the health check ID.

Request

None

Response

Table 6-139 Parameter description

Parameter	Type	Description
healthmonitor	**Healthmonitor** object	Specifies the health check. For details, see **Table 6-140**.

Table 6-140 healthmonitor parameter description

Parameter	Type	Description
id	String	Specifies the health check ID.
tenant_id	String	Specifies the ID of the project where the health check is performed.
project_id	String	Specifies the ID of the project to which the health check belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the health check name.

Parameter	Type	Description
delay	Integer	Specifies the maximum time between health checks in the unit of second. The value ranges from **1** to **50**.
max_retries	Integer	Specifies the maximum number of retries. The value ranges from **1** to **10**.
max_retries_down	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **ONLINE** to **OFFLINE**. The value ranges from **1** to **10**.
pools	Array of **Pools** objects	Lists the IDs of backend server groups associated with the health check. For details, see **Table 6-132**.
admin_state_up	Boolean	Specifies the administrative status of the health check. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
timeout	Integer	Specifies the health check timeout duration in the unit of second. The value ranges from **1** to **50**. **NOTE** You are advised to set the value less than that of parameter **delay**.
type	String	Specifies the health check protocol. The value can be **TCP**, **UDP_CONNECT**, or **HTTP**.
monitor_port	Integer	Specifies the health check port. The port number ranges from 1 to 65535. The value is left blank by default, indicating that the port of the backend server is used as the health check port.
expected_codes	String	Specifies the expected HTTP status code. The following options are available: A single value, such as **200** A list of values, such as **200,202** A value range, such as **200–204** This parameter takes effect only when the value of **type** is set to **HTTP**. Currently, this parameter is not supported and is fixed at **200**.

Parameter	Type	Description
domain_name	String	Specifies the domain name of HTTP requests during the health check. This parameter takes effect only when the value of **type** is set to **HTTP**. The value is left blank by default, indicating that the private IP address of the load balancer is used as the destination address of HTTP requests. The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter, for example: www.test.com.
url_path	String	Specifies the HTTP request path for the health check. The default value is **/**. The value starts with a slash (/). This parameter takes effect only when the value of **type** is set to **HTTP**. An example value is **/test**.
http_method	String	Specifies the HTTP request method. The default value is **GET**. The value can be **GET**, **HEAD**, **POST**, **PUT**, **DELETE**, **TRACE**, **OPTIONS**, **CONNECT**, or **PATCH**. This parameter takes effect only when the value of **type** is set to **HTTP**. **NOTE** This parameter is reserved.

Table 6-141 pools parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	Specifies the ID of the backend server group.

Example Request

- Example request: Querying details of a health check
  ```
  GET https://{endpoint}/v2/145483a5107745e9b3d80f956713e6a3/elb/healthmonitors/b7633ade-24dc-4d72-8475-06aa22be5412
  ```

Example Response

- Example response 1
  ```
  {
    "healthmonitor": {
  ```



```
  "name": "",
  "admin_state_up": true,
  "tenant_id": "145483a5107745e9b3d80f956713e6a3",
  "project_id": "145483a5107745e9b3d80f956713e6a3",
  "domain_name": null,
  "delay": 10,
  "expected_codes": "200",
  "max_retries": 10,
  "http_method": "GET",
  "timeout": 10,
  "pools": [
    {
      "id": "bb44bffb-05d9-412c-9d9c-b189d9e14193"
    }
  ],
  "url_path": "/",
  "type": "HTTP",
  "id": "61c24cba-19bb-45c1-a013-7565e5f98872",
  "monitor_port": 112
 }
}
```


Status Code

For details, see **Status Codes**.

6.5.4 Updating a Health Check

Function

This API is used to update a health check.

Constraints

If **provisioning_status** of the load balancer for which the health check is configured is not **ACTIVE**, the health check cannot be updated.

URI

PUT /v2/{project_id}/elb/healthmonitors/{healthmonitor_id}

Table 6-142 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
healthmonitor_id	Yes	String	Specifies the health check ID.

Request

Table 6-143 Parameter description

Parameter	Mandatory	Type	Description
healthmonitor	Yes	**Healthmonitor** object	Specifies the health check. For details, see **Table 6-144**.

Table 6-144 healthmonitor parameter description

Parameter	Mandatory	Type	Description
name	No	String	Specifies the health check name. The value contains a maximum of 255 characters.
delay	No	Integer	Specifies the maximum time between health checks in the unit of second. The value ranges from **1** to **50**.
max_retries	No	Integer	Specifies the maximum number of retries. The value ranges from **1** to **10**.
admin_state_up	No	Boolean	Specifies the administrative status of the health check. This parameter is reserved, and the default value is **true**.
timeout	No	Integer	Specifies the health check timeout duration in the unit of second. The value ranges from **1** to **50**. **NOTE** You are advised to set the value less than that of parameter **delay**.
type	No	String	Specifies the health check protocol. The value can be **TCP**, **UDP_CONNECT**, or **HTTP**.
monitor_port	No	Integer	Specifies the health check port. The port number ranges from 1 to 65535. The value is left blank by default, indicating that the port of the backend server is used as the health check port.

Parameter	Mandatory	Type	Description
expected_codes	No	String	Specifies the expected HTTP status code. The following options are available: A single value, such as **200** A list of values, such as **200,202** A value range, such as **200–204** This parameter takes effect only when the value of **type** is set to **HTTP**.
domain_name	No	String	Specifies the domain name of HTTP requests during the health check. This parameter takes effect only when the value of **type** is set to **HTTP**. The value is left blank by default, indicating that the private IP address of the load balancer is used as the destination address of HTTP requests. The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter, for example: www.test.com. The value contains a maximum of 100 characters.
url_path	No	String	Specifies the HTTP request path for the health check. The default value is **/**. The value starts with a slash (/). This parameter takes effect only when the value of **type** is set to **HTTP**. An example value is **/test**. The value contains a maximum of 80 characters.
http_method	No	String	Specifies the HTTP request method. The default value is **GET**. The value can be **GET**, **HEAD**, **POST**, **PUT**, **DELETE**, **TRACE**, **OPTIONS**, **CONNECT**, or **PATCH**. This parameter takes effect only when the value of **type** is set to **HTTP**. **NOTE** This parameter is reserved.

Response

Table 6-145 Parameter description

Parameter	Type	Description
healthmonitor	**Healthmonitor** object	Specifies the health check. For details, see **Table 6-146**.

Table 6-146 healthmonitor parameter description

Parameter	Type	Description
id	String	Specifies the health check ID.
tenant_id	String	Specifies the ID of the project where the health check is performed.
project_id	String	Specifies the ID of the project to which the health check belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the health check name.
delay	Integer	Specifies the maximum time between health checks in the unit of second. The value ranges from **1** to **50**.
max_retries	Integer	Specifies the maximum number of retries. The value ranges from **1** to **10**.
max_retries_down	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **ONLINE** to **OFFLINE**. The value ranges from **1** to **10**.
pools	Array of **Pools** objects	Lists the IDs of backend server groups associated with the health check. For details, see **Table 6-132**.
admin_state_up	Boolean	Specifies the administrative status of the health check. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
timeout	Integer	Specifies the health check timeout duration in the unit of second. The value ranges from **1** to **50**. **NOTE** You are advised to set the value less than that of parameter **delay**.

Parameter	Type	Description
type	String	Specifies the health check protocol. The value can be **TCP**, **UDP_CONNECT**, or **HTTP**.
monitor_port	Integer	Specifies the health check port. The port number ranges from 1 to 65535. The value is left blank by default, indicating that the port of the backend server is used as the health check port.
expected_codes	String	Specifies the expected HTTP status code. The following options are available: A single value, such as **200** A list of values, such as **200,202** A value range, such as **200–204** This parameter takes effect only when the value of **type** is set to **HTTP**. Currently, this parameter is not supported and is fixed at **200**.
domain_name	String	Specifies the domain name of HTTP requests during the health check. This parameter takes effect only when the value of **type** is set to **HTTP**. The value is left blank by default, indicating that the private IP address of the load balancer is used as the destination address of HTTP requests. The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter, for example: www.test.com.
url_path	String	Specifies the HTTP request path for the health check. The default value is **/**. The value starts with a slash (/). This parameter takes effect only when the value of **type** is set to **HTTP**. An example value is **/test**.

Parameter	Type	Description
http_method	String	Specifies the HTTP request method. The default value is **GET**. The value can be **GET**, **HEAD**, **POST**, **PUT**, **DELETE**, **TRACE**, **OPTIONS**, **CONNECT**, or **PATCH**. This parameter takes effect only when the value of **type** is set to **HTTP**. **NOTE** This parameter is reserved.

Table 6-147 pools parameter description

Parameter	Mandatory	Type	Description
id	Yes	String	Specifies the ID of the backend server group.

Example Request

- Example request: Updating a health check

```
PUT https://{endpoint}/v2/145483a5107745e9b3d80f956713e6a3/elb/healthmonitors/
b7633ade-24dc-4d72-8475-06aa22be5412

{
  "healthmonitor": {
    "delay": 15,
    "name": "health-xx",
    "timeout": 12
  }
}
```

Example Response

- Example response

```
{
  "healthmonitor": {
    "name": "health-xx",
    "admin_state_up": true,
    "tenant_id": "145483a5107745e9b3d80f956713e6a3",
    "project_id": "145483a5107745e9b3d80f956713e6a3",
    "domain_name": null,
    "delay": 15,
    "expected_codes": "200",
    "max_retries": 10,
    "http_method": "GET",
    "timeout": 12,
    "pools": [
      {
        "id": "bb44bffb-05d9-412c-9d9c-b189d9e14193"
      }
    ],
    "url_path": "/",
    "type": "HTTP",
    "id": "2dca3867-98c5-4cde-8f2c-b89ae6bd7e36",
```



```
    "monitor_port": 112
  }
}
```

Status Code

For details, see **Status Codes**.

6.5.5 Deleting a Health Check

Function

This API is used to delete a health check.

Constraints

If **provisioning_status** of the load balancer for which the health check is configured is not **ACTIVE**, the health check cannot be deleted.

URI

DELETE /v2/{project_id}/elb/healthmonitors/{healthmonitor_id}

Table 6-148 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
healthmonitor_id	Yes	String	Specifies the health check ID.

Request

None

Response

None

Example Request

- Example request: Deleting a health check

```
DELETE https://{Endpoint}/v2/145483a5107745e9b3d80f956713e6a3/elb/healthmonitors/b7633ade-24dc-4d72-8475-06aa22be5412
```

Example Response

- Example response

  None

Status Code

For details, see **Status Codes**.

6.6 Forwarding Policy

6.6.1 Adding a Forwarding Policy

Function

This API is used to add a forwarding policy. The listener and forwarding policy determine how traffic is forwarded to backend servers.

- By matching the URL or domain name specified in the forwarding policy when **action** is set to **REDIRECT_TO_POOL**, the load balancer distributes the traffic to backend servers in a specific backend server group.
- When **action** is set to **REDIRECT_TO_LISTENER**, the HTTP listener is redirected to an HTTPS listener, and requests are routed by the HTTPS listener.

Constraints

Currently, only redirects from an HTTP listener to an HTTPS listener are supported. When **action** is set to **REDIRECT_TO_LISTENER**, the listener specified by **listener_id** can only be an HTTP listener, and the listener specified by **redirect_listener_id** can only be an HTTPS listener.

The load balancer of the HTTPS listener to which traffic is redirected must be the same as that of the HTTP listener.

URI

POST /v2/{project_id}/elb/l7policies

Table 6-149 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Request

Table 6-150 Parameter description

Parameter	Mandatory	Type	Description
l7policy	Yes	**L7policy** object	Specifies the forwarding policy. For details, see **Table 6-151**.

Table 6-151 l7policy parameter description

Parameter	Mandatory	Type	Description
tenant_id	No	String	Specifies the ID of the project where the forwarding policy is used. The value must be the same as the value of **project_id** in the token. The value contains a maximum of 255 characters.
name	No	String	Specifies the forwarding policy name. The value contains a maximum of 255 characters.
admin_state_up	No	Boolean	Specifies the administrative status of the forwarding policy. The value can only be **true**.
description	No	String	Provides supplementary information about the forwarding policy. The value contains a maximum of 255 characters.
listener_id	Yes	String	Specifies the ID of the listener for which the forwarding policy is added. • When **action** is set to **REDIRECT_TO_POOL**, forwarding policies can be added to a listener with **protocol** set to **HTTP** or **TERMINATED_HTTPS**. • When **action** is set to **REDIRECT_TO_LISTENER**, forwarding policies can be added to a listener with **protocol** set to **HTTP**.
action	Yes	String	Specifies whether requests are forwarded to another backend server group or redirected to an HTTPS listener. The value can be: • **REDIRECT_TO_POOL**: Requests are forwarded to the backend server group specified by **redirect_pool_id**. • **REDIRECT_TO_LISTENER**: Requests are redirected from the HTTP listener specified by **listener_id** to the HTTPS listener specified by **redirect_listener_id**.

Parameter	Mandatory	Type	Description
redirect_pool_id	No	String	Specifies the ID of the backend server group to which traffic is forwarded. The default value is **null**. This parameter is mandatory when **action** is set to **REDIRECT_TO_POOL**. This parameter cannot be specified when **action** is set to **REDIRECT_TO_LISTENER**. The backend server group must meet the following requirements: • Cannot be the default backend server group of the listener. • Cannot be the backend server group used by forwarding policies of other listeners.
redirect_listener_id	No	String	Specifies the ID of the listener to which the traffic is redirected. The default value is **null**. This parameter is mandatory when **action** is set to **REDIRECT_TO_LISTENER**. This parameter cannot be specified when **action** is set to **REDIRECT_TO_POOL**. The listener must meet the following requirements: • Can only be an HTTPS listener. • Can only be a listener of the same load balancer.
redirect_url	No	String	Specifies the URL to which traffic is redirected. The default value is **null**. This parameter is reserved. The value contains a maximum of 255 characters.
position	No	Integer	Specifies the forwarding priority. The value ranges from **1** to **100**. The default value is **100**. This parameter is reserved.

Parameter	Mandatory	Type	Description
rules	No	Array of **Rules** objects	Lists the forwarding rules of the forwarding policy. For details, see **Table 6-152**. The list contains a maximum of two rules, and the **type** parameter of each rule must be unique.

Table 6-152 rules parameter description

Parameter	Type	Mandatory	Description
admin_state_up	Boolean	No	Specifies the administrative status of the forwarding rule. The value can only be **true**.
type	String	Yes	Specifies the match type of a forwarding rule. The value can be: • **HOST_NAME**: matches the domain name in the request. • **PATH**: matches the path in the request. The match type of forwarding rules in a forwarding policy must be unique.
compare_type	String	Yes	Specifies the match mode. The options are as follows: When **type** is set to **HOST_NAME**, the value of this parameter can only be the following: • **EQUAL_TO**: indicates exact match. When **type** is set to **PATH**, the value of this parameter can be one of the following: • **REGEX**: indicates regular expression match. • **STARTS_WITH**: indicates prefix match. • **EQUAL_TO**: indicates exact match.

Parameter	Type	Mandatory	Description
invert	Boolean	No	Specifies whether reverse matching is supported. The value can be **true** or **false**. The default value is **false**. This parameter is reserved.
key	String	No	Specifies the key of the match content. The default value is **null**. This parameter is reserved.
value	String	Yes	Specifies the value of the match content. The value cannot contain spaces. • When **type** is set to **HOST_NAME**, the value can contain a maximum of 100 characters that contain only letters, digits, hyphens (-), and periods (.), and must start with a letter or digit. • When **type** is set to **PATH**, the value can contain a maximum of 128 characters. When **compare_type** is set to **STARTS_WITH** or **EQUAL_TO**, the value must start with a slash (/) and can contain only letters, digits, and special characters _~';@^-%#&$.*+?,=!:| \/()[]{}

Response

Table 6-153 Parameter description

Parameter	Type	Description
l7policy	**L7policy** object	Specifies the forwarding policy. For details, see **Table 6-154**.

Table 6-154 l7policy parameter description

Parameter	Type	Description
id	String	Specifies the forwarding policy ID.

Parameter	Type	Description
tenant_id	String	Specifies the ID of the project where the forwarding policy is used.
project_id	String	Specifies the ID of the project to which the forwarding policy belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the forwarding policy name.
admin_state_up	Boolean	Specifies the administrative status of the forwarding policy. The value can only be **true**.
description	String	Provides supplementary information about the forwarding policy.
listener_id	String	Specifies the ID of the listener to which the forwarding policy is added.
action	String	Specifies whether requests are forwarded to another backend server group or redirected to an HTTPS listener. The value can be: • **REDIRECT_TO_POOL**: Requests are forwarded to the backend server group specified by **redirect_pool_id**. • **REDIRECT_TO_LISTENER**: Requests are redirected from the HTTP listener specified by **listener_id** to the HTTPS listener specified by **redirect_listener_id**.
redirect_pool_id	String	Specifies the ID of the backend server group to which traffic is forwarded.
redirect_listener_id	String	Specifies the ID of the listener to which the traffic is redirected.
redirect_url	String	Specifies the URL to which traffic is redirected. This parameter is reserved.
rules	Array of **Rules** objects	Lists the forwarding rules of the forwarding policy. For details, see **Table 6-155**.
position	Integer	Specifies the forwarding priority. The value ranges from **1** to **100**. The default value is **100**. This parameter is reserved.
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the forwarding policy.

Table 6-155 rules parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated forwarding rule.

Example Request

- Example request 1: Adding a forwarding policy

```
POST https://{Endpoint}/v2/573d73c9f90e48d0bddfa0eb202b25c2/elb/l7policies

{
   "l7policy": {
      "name": "niubiao_yaqing_api-2",
      "listener_id": "3e24a3ca-11e5-4aa3-abd4-61ba0a8a18f1",
      "action": "REDIRECT_TO_POOL",
      "redirect_pool_id": "6460f13a-76de-43c7-b776-4fefc06a676e",
      "rules": [
         {
            "type": "PATH",
            "compare_type": "EQUAL_TO",
            "value": "/test"
         },
         {
            "type": "HOST_NAME",
            "compare_type": "EQUAL_TO",
            "value": "www.test.com"
         }
      ]
   }
}
```

Example Response

- Example response 1

```
{
   "l7policy": {
      "redirect_pool_id": "6460f13a-76de-43c7-b776-4fefc06a676e",
      "description": "",
      "admin_state_up": true,
      "rules": [
         {
            "id": "742600d9-2a14-4808-af69-336883dbb590"
         },
         {
            "id": "3251ed77-0d52-412b-9310-733636bb3fbf"
         }
      ],
      "tenant_id": "573d73c9f90e48d0bddfa0eb202b25c2",
      "listener_id": "3e24a3ca-11e5-4aa3-abd4-61ba0a8a18f1",
      "redirect_url": null,
      "redirect_listener_id": null,
      "action": "REDIRECT_TO_POOL",
      "position": 100,
      "provisioning_status": "ACTIVE",
      "project_id": "573d73c9f90e48d0bddfa0eb202b25c2",
      "id": "65d6e115-f179-4bcd-9bbb-1484e5f8ee81",
      "name": "niubiao_yaqing-_api-2"
   }
}
```


Status Code

For details, see **Status Codes**.

6.6.2 Querying Forwarding Policies

Function

This API is used to query all the forwarding policies. Filter query and pagination query are supported. Unless otherwise specified, exact match is applied.

URI

GET /v2/{project_id}/elb/l7policies

Table 6-156 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Table 6-157 Query parameters

Parameter	Mandatory	Type	Description
marker	No	String	Specifies the ID of the forwarding policy from which pagination query starts, that is, the ID of the last forwarding policy on the previous page. This parameter must be used together with **limit**.
limit	No	Integer	Specifies the number of forwarding policies on each page. If this parameter is not set, all forwarding policies are queried by default.
page_reverse	No	Boolean	Specifies the page direction. The value can be **true** or **false**, and the default value is **false**. The last page in the list requested with **page_reverse** set to **false** will not contain the "next" link, and the last page in the list requested with **page_reverse** set to **true** will not contain the "previous" link. This parameter must be used together with **limit**.

Parameter	Mandatory	Type	Description
id	No	String	Specifies the forwarding policy ID.
tenant_id	No	String	Specifies the ID of the project where the forwarding policy is used. The value contains a maximum of 255 characters.
project_id	No	String	Specifies the ID of the project to which the forwarding policy belongs. This parameter has the same meaning as **tenant_id**.
name	No	String	Specifies the forwarding policy name. The value contains a maximum of 255 characters.
admin_state_up	No	Boolean	Specifies the administrative status of the forwarding policy.
description	No	String	Provides supplementary information about the forwarding policy. The value contains a maximum of 255 characters.
listener_id	No	String	Specifies the ID of the listener to which the forwarding policy is added.
action	No	String	Specifies whether requests are forwarded to another backend server group or redirected to an HTTPS listener. The value can be: • **REDIRECT_TO_POOL**: Requests are forwarded to the backend server group specified by **redirect_pool_id**. • **REDIRECT_TO_LISTENER**: Requests are redirected from the HTTP listener specified by **listener_id** to the HTTPS listener specified by **redirect_listener_id**.
redirect_pool_id	No	String	Specifies the ID of the backend server group to which traffic is forwarded.
redirect_listener_id	No	String	Specifies the ID of the listener to which the traffic is redirected.

Parameter	Mandatory	Type	Description
redirect_url	No	String	Specifies the URL to which traffic is redirected. This parameter is reserved. The value contains a maximum of 255 characters.
position	No	Integer	Specifies the forwarding priority. The value ranges from **1** to **100**. The default value is **100**. This parameter is reserved.
provisioning_status	No	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the forwarding policy.
enterprise_project_id	No	String	Specifies the enterprise project ID. Enterprise projects are used for fine-grained authentication. • If **listener_id** is passed, the ID of the enterprise project to which the load balancer belongs is used for authentication. • If **listener_id** is not passed, the ID of the enterprise project to which the forwarding policy belongs is used for authentication. • If neither **listener_id** nor **enterprise_project_id** is passed, fine-grained authentication is performed. The **elb:loadbalancers:list** permissions must be assigned to the user group.

Request

None

Response

Table 6-158 Response parameters

Parameter	Type	Description
l7policies	Array of **L7policies** objects	Lists the forwarding policies. For details, see **Table 6-159**.

Table 6-159 l7policy parameter description

Parameter	Type	Description
id	String	Specifies the forwarding policy ID.
tenant_id	String	Specifies the ID of the project where the forwarding policy is used.
project_id	String	Specifies the ID of the project to which the forwarding policy belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the forwarding policy name.
admin_state_up	Boolean	Specifies the administrative status of the forwarding policy. The value can only be **true**.
description	String	Provides supplementary information about the forwarding policy.
listener_id	String	Specifies the ID of the listener to which the forwarding policy is added.
action	String	Specifies whether requests are forwarded to another backend server group or redirected to an HTTPS listener. The value can be: • **REDIRECT_TO_POOL**: Requests are forwarded to the backend server group specified by **redirect_pool_id**. • **REDIRECT_TO_LISTENER**: Requests are redirected from the HTTP listener specified by **listener_id** to the HTTPS listener specified by **redirect_listener_id**.
redirect_pool_id	String	Specifies the ID of the backend server group to which traffic is forwarded.
redirect_listener_id	String	Specifies the ID of the listener to which the traffic is redirected.

Parameter	Type	Description
redirect_url	String	Specifies the URL to which traffic is redirected. This parameter is reserved.
rules	Array of **Rules** objects	Lists the forwarding rules of the forwarding policy. For details, see **Table 6-155**.
position	Integer	Specifies the forwarding priority. The value ranges from **1** to **100**. The default value is **100**. This parameter is reserved.
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the forwarding policy.

Table 6-160 rules parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated forwarding rule.

Example Request

- Example request 1: Querying all forwarding policies
  ```
  GET https://{Endpoint}/v2/a31d2bdcf7604c0faaddb058e1e08819/elb/l7policies
  ```
- Example request 2: Querying forwarding policies through which requests are forwarded to the backend server group
  ```
  GET https://{Endpoint}/v2/a31d2bdcf7604c0faaddb058e1e08819/elb/l7policies?
  action=REDIRECT_TO_POOL
  ```

Example Response

- Example response 1
  ```
  {
    "l7policies": [
      {
        "redirect_pool_id": "431a03eb-81bb-408e-ae37-7ce19023692b",
        "redirect_listener_id": null,
        "description": "",
        "admin_state_up": true,
        "rules": [
          {
            "id": "67d8a8fa-b0dd-4bd4-a85b-671db19b2ef3"
          },
          {
            "id": "f02b3bca-69d2-4335-a3fa-a8054e996213"
          }
        ],
        "tenant_id": "a31d2bdcf7604c0faaddb058e1e08819",
        "project_id": "a31d2bdcf7604c0faaddb058e1e08819",
  ```



```
            "listener_id": "26058b64-6185-4e06-874e-4bd68b7633d0",
            "redirect_url": null,
            "action": "REDIRECT_TO_POOL",
            "position": 2,
            "provisioning_status": "ACTIVE",
            "id": "5ae0e1e7-5f0f-47a1-b39f-5d4c428a1586",
            "name": ""
        },
        {
            "redirect_pool_id": "59eebd7b-c68f-4f8a-aa7f-e062e84c0690",
            "redirect_listener_id": null,
            "description": "",
            "admin_state_up": true,
            "rules": [
                {
                    "id": "f4499f48-de3d-4efe-926d-926aa4d6aaf5"
                }
            ],
            "tenant_id": "a31d2bdcf7604c0faaddb058e1e08819",
            "project_id": "a31d2bdcf7604c0faaddb058e1e08819",
            "listener_id": "e1310063-00de-4867-ab55-ccac4d9db364",
            "redirect_url": null,
            "action": "REDIRECT_TO_POOL",
            "position": 1,
            "provisioning_status": "ACTIVE",
            "id": "6cfd9d89-1d7e-4d84-ae1f-a8c5ff126f72",
            "name": ""
        }
    ]
}
```


- Example response 2


```
{
    "l7policies": [
        {
            "redirect_pool_id": "431a03eb-81bb-408e-ae37-7ce19023692b",
            "redirect_listener_id": null,
            "description": "",
            "admin_state_up": true,
            "rules": [
                {
                    "id": "67d8a8fa-b0dd-4bd4-a85b-671db19b2ef3"
                },
                {
                    "id": "f02b3bca-69d2-4335-a3fa-a8054e996213"
                }
            ],
            "tenant_id": "a31d2bdcf7604c0faaddb058e1e08819",
            "project_id": "a31d2bdcf7604c0faaddb058e1e08819",
            "listener_id": "26058b64-6185-4e06-874e-4bd68b7633d0",
            "redirect_url": null,
            "action": "REDIRECT_TO_POOL",
            "position": 2,
            "provisioning_status": "ACTIVE",
            "id": "5ae0e1e7-5f0f-47a1-b39f-5d4c428a1586",
            "name": ""
        },
        {
            "redirect_pool_id": "59eebd7b-c68f-4f8a-aa7f-e062e84c0690",
            "redirect_listener_id": null,
            "description": "",
            "admin_state_up": true,
            "rules": [
                {
                    "id": "f4499f48-de3d-4efe-926d-926aa4d6aaf5"
                }
            ],
            "tenant_id": "a31d2bdcf7604c0faaddb058e1e08819",
            "project_id": "a31d2bdcf7604c0faaddb058e1e08819",
            "listener_id": "e1310063-00de-4867-ab55-ccac4d9db364",
```



```
        "redirect_url": null,
        "action": "REDIRECT_TO_POOL",
        "position": 1,
        "provisioning_status": "ACTIVE",
        "id": "6cfd9d89-1d7e-4d84-ae1f-a8c5ff126f72",
        "name": ""
      }
    ]
}
```


Status Code

For details, see **Status Codes**.

6.6.3 Querying Details of a Forwarding Policy

Function

This API is used to query details about a forwarding policy.

URI

GET /v2/{project_id}/elb/l7policies/{l7policy_id}

Table 6-161 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
l7policy_id	Yes	String	Specifies the forwarding policy ID.

Request

None

Response

Table 6-162 Parameter description

Parameter	Type	Description
l7policy	**L7policy** object	Specifies the forwarding policy. For details, see **Table 6-163**.

Table 6-163 l7policy parameter description

Parameter	Type	Description
id	String	Specifies the forwarding policy ID.
tenant_id	String	Specifies the ID of the project where the forwarding policy is used.
project_id	String	Specifies the ID of the project to which the forwarding policy belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the forwarding policy name.
admin_state_up	Boolean	Specifies the administrative status of the forwarding policy. The value can only be **true**.
description	String	Provides supplementary information about the forwarding policy.
listener_id	String	Specifies the ID of the listener to which the forwarding policy is added.
action	String	Specifies whether requests are forwarded to another backend server group or redirected to an HTTPS listener. The value can be: • **REDIRECT_TO_POOL**: Requests are forwarded to the backend server group specified by **redirect_pool_id**. • **REDIRECT_TO_LISTENER**: Requests are redirected from the HTTP listener specified by **listener_id** to the HTTPS listener specified by **redirect_listener_id**.
redirect_pool_id	String	Specifies the ID of the backend server group to which traffic is forwarded.
redirect_listener_id	String	Specifies the ID of the listener to which the traffic is redirected.
redirect_url	String	Specifies the URL to which traffic is redirected. This parameter is reserved.
rules	Array of **Rules** objects	Lists the forwarding rules of the forwarding policy. For details, see **Table 6-155**.
position	Integer	Specifies the forwarding priority. The value ranges from **1** to **100**. The default value is **100**. This parameter is reserved.

Parameter	Type	Description
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the forwarding policy.

Table 6-164 rules parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated forwarding rule.

Example Request

- Example request: Querying details of a forwarding policy
  GET https://{Endpoint}/v2/a31d2bdcf7604c0faaddb058e1e08819/elb/l7policies/5ae0e1e7-5f0f-47a1-b39f-5d4c428a1586

Example Response

- Example response 1

```
{
    "l7policy": {
        "redirect_pool_id": "431a03eb-81bb-408e-ae37-7ce19023692b",
        "redirect_listener_id": null,
        "description": "",
        "admin_state_up": true,
        "rules": [
            {
                "id": "67d8a8fa-b0dd-4bd4-a85b-671db19b2ef3"
            },
            {
                "id": "f02b3bca-69d2-4335-a3fa-a8054e996213"
            }
        ],
        "tenant_id": "a31d2bdcf7604c0faaddb058e1e08819",
        "project_id": "a31d2bdcf7604c0faaddb058e1e08819",
        "listener_id": "26058b64-6185-4e06-874e-4bd68b7633d0",
        "redirect_url": null,
        "provisioning_status": "ACTIVE",
        "action": "REDIRECT_TO_POOL",
        "position": 1,
        "id": "5ae0e1e7-5f0f-47a1-b39f-5d4c428a1586",
        "name": "l7policy-garry-1"
    }
}
```

Status Code

For details, see **Status Codes**.

6.6.4 Updating a Forwarding Policy

Function

This API is used to update a forwarding policy.

URI

PUT /v2/{project_id}/elb/l7policies/{l7policy_id}

Table 6-165 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
l7policy_id	Yes	String	Specifies the forwarding policy ID.

Request

Table 6-166 Parameter description

Parameter	Mandatory	Type	Description
l7policy	Yes	**L7policy** object	Specifies the forwarding policy. For details, see **Table 6-167**.

Table 6-167 l7policy parameter description

Parameter	Mandatory	Type	Description
name	No	String	Specifies the forwarding policy name. The value contains a maximum of 255 characters.
description	No	String	Provides supplementary information about the forwarding policy. The value contains a maximum of 255 characters.

Parameter	Mandatory	Type	Description
redirect_pool_id	No	String	Specifies the ID of the backend server group to which traffic is forwarded. The default value is **null**. This parameter is mandatory when **action** is set to **REDIRECT_TO_POOL**. This parameter cannot be specified when **action** is set to **REDIRECT_TO_LISTENER**. The backend server group must meet the following requirements: • Cannot be the default backend server group of the listener. • Cannot be the backend server group used by forwarding policies of other listeners.
redirect_listener_id	No	String	Specifies the ID of the listener to which the traffic is redirected. The default value is **null**. This parameter is mandatory when **action** is set to **REDIRECT_TO_LISTENER**. This parameter cannot be specified when **action** is set to **REDIRECT_TO_POOL**. The listener must meet the following requirements: • Can only be an HTTPS listener. • Can only be a listener of the same load balancer.
admin_state_up	No	Boolean	Specifies the administrative status of the forwarding policy. The value can only be **true**.

Response

Table 6-168 Parameter description

Parameter	Type	Description
l7policy	**L7policy** object	Specifies the forwarding policy. For details, see **Table 6-169**.

Table 6-169 l7policy parameter description

Parameter	Type	Description
id	String	Specifies the forwarding policy ID.
tenant_id	String	Specifies the ID of the project where the forwarding policy is used.
project_id	String	Specifies the ID of the project to which the forwarding policy belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the forwarding policy name.
admin_state_up	Boolean	Specifies the administrative status of the forwarding policy. The value can only be **true**.
description	String	Provides supplementary information about the forwarding policy.
listener_id	String	Specifies the ID of the listener to which the forwarding policy is added.
action	String	Specifies whether requests are forwarded to another backend server group or redirected to an HTTPS listener. The value can be: • **REDIRECT_TO_POOL**: Requests are forwarded to the backend server group specified by **redirect_pool_id**. • **REDIRECT_TO_LISTENER**: Requests are redirected from the HTTP listener specified by **listener_id** to the HTTPS listener specified by **redirect_listener_id**.
redirect_pool_id	String	Specifies the ID of the backend server group to which traffic is forwarded.
redirect_listener_id	String	Specifies the ID of the listener to which the traffic is redirected.
redirect_url	String	Specifies the URL to which traffic is redirected. This parameter is reserved.
rules	Array of **Rules** objects	Lists the forwarding rules of the forwarding policy. For details, see **Table 6-155**.
position	Integer	Specifies the forwarding priority. The value ranges from **1** to **100**. The default value is **100**. This parameter is reserved.

Parameter	Type	Description
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the forwarding policy.

Table 6-170 rules parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated forwarding rule.

Example Request

- Example request: Updating a forwarding policy

```
PUT https://{Endpoint}/v2/a31d2bdcf7604c0faaddb058e1e08819/elb/l7policies/5ae0e1e7-5f0f-47a1-b39f-5d4c428a1586

{
    "l7policy": {
        "name": "test"
    }
}
```

Example Response

- Example response

```
{
    "l7policy": {
        "redirect_pool_id": "431a03eb-81bb-408e-ae37-7ce19023692b",
        "redirect_listener_id": null,
        "description": "",
        "admin_state_up": true,
        "rules": [
            {
                "id": "67d8a8fa-b0dd-4bd4-a85b-671db19b2ef3"
            },
            {
                "id": "f02b3bca-69d2-4335-a3fa-a8054e996213"
            }
        ],

        "tenant_id": "a31d2bdcf7604c0faaddb058e1e08819",
        "project_id": "a31d2bdcf7604c0faaddb058e1e08819",
        "listener_id": "26058b64-6185-4e06-874e-4bd68b7633d0",
        "redirect_url": null,
        "action": "REDIRECT_TO_POOL",
        "position": 2,
        "provisioning_status": "ACTIVE",
        "id": "5ae0e1e7-5f0f-47a1-b39f-5d4c428a1586",
        "name": "test"
    }
}
```


Status Code

For details, see **Status Codes**.

6.6.5 Deleting a Forwarding Policy

Function

This API is used to delete a forwarding policy.

URI

DELETE /v2/{project_id}/elb/l7policies/{l7policy_id}

Table 6-171 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
l7policy_id	Yes	String	Specifies the forwarding policy ID.

Request

None

Response

None

Example Request

- Example request: Deleting a forwarding policy
  ```
  DELETE https://{Endpoint}/v2/a31d2bdcf7604c0faaddb058e1e08819/elb/l7policies/5ae0e1e7-5f0f-47a1-b39f-5d4c428a1586
  ```

Example Response

- Example response

  None

Status Code

For details, see **Status Codes**.

6.7 Forwarding Rule

6.7.1 Adding a Forwarding Rule

Function

This API is used to add a forwarding rule. After you add a forwarding rule, the load balancer matches the domain name and path in the request and distributes the traffic to the backend server group specified by **redirect_pool_id** of the associated forwarding policy.

Constraints

The match type of forwarding rules in a forwarding policy must be unique.

URI

POST /v2/{project_id}/elb/l7policies/{l7policy_id}/rules

Table 6-172 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
l7policy_id	Yes	String	Specifies the forwarding policy ID.

Request

Table 6-173 Parameter description

Parameter	Mandatory	Type	Description
rule	Yes	**Rule** object	Specifies the forwarding rule. For details, see **Table 6-174**.

Table 6-174 rule parameter description

Parameter	Mandatory	Type	Description
tenant_id	No	String	Specifies the ID of the project where the forwarding rule is used. The value must be the same as the value of **project_id** in the token. The value contains a maximum of 255 characters.
admin_state_up	No	Boolean	Specifies the administrative status of the forwarding rule. The value can only be **true**.
type	Yes	String	Specifies the match type of a forwarding rule. The value can be: • **HOST_NAME**: matches the domain name in the request. • **PATH**: matches the path in the request. The match type of forwarding rules in a forwarding policy must be unique.
compare_type	Yes	String	Specifies the match mode. The options are as follows: When **type** is set to **HOST_NAME**, the value of this parameter can only be the following: • **EQUAL_TO**: indicates exact match. When **type** is set to **PATH**, the value of this parameter can be one of the following: • **REGEX**: indicates regular expression match. • **STARTS_WITH**: indicates prefix match. • **EQUAL_TO**: indicates exact match.
invert	No	Boolean	Specifies whether reverse matching is supported. The value can be **true** or **false**. The default value is **false**. This parameter is reserved.

Parameter	Mandatory	Type	Description
key	No	String	Specifies the key of the match content. The default value is **null**. This parameter is reserved. The value contains a maximum of 255 characters.
value	Yes	String	Specifies the value of the match content. The value cannot contain spaces. The value contains a maximum of 128 characters. • When **type** is set to **HOST_NAME**, the value can contain a maximum of 100 characters that contain only letters, digits, hyphens (-), and periods (.), and must start with a letter or digit. • When **type** is set to **PATH**, the value can contain a maximum of 128 characters. When **compare_type** is set to **STARTS_WITH** or **EQUAL_TO**, the value must start with a slash (/) and can contain only letters, digits, and special characters _~';@^-%#&$.*+?,=!:|\/()[]{}

Response

Table 6-175 Parameter description

Parameter	Type	Description
rule	**Rule** object	Specifies the forwarding rule. For details, see **Table 6-176**.

Table 6-176 rule parameter description

Parameter	Type	Description
id	String	Specifies the forwarding rule ID.

Parameter	Type	Description
tenant_id	String	Specifies the ID of the project where the forwarding rule is used. The value contains a maximum of 255 characters.
project_id	String	Specifies the ID of the project to which the forwarding rule belongs. This parameter has the same meaning as **tenant_id**.
admin_state_up	Boolean	Specifies the administrative status of the forwarding rule. The value can only be **true**.
type	String	Specifies the match type of a forwarding rule. The value can be: • **HOST_NAME**: matches the domain name in the request. • **PATH**: matches the path in the request.
compare_type	String	Specifies the match mode. The options are as follows: When **type** is set to **HOST_NAME**, the value of this parameter can only be the following: • **EQUAL_TO**: indicates exact match. When **type** is set to **PATH**, the value of this parameter can be one of the following: • **REGEX**: indicates regular expression match. • **STARTS_WITH**: indicates prefix match. • **EQUAL_TO**: indicates exact match.
invert	Boolean	Specifies whether reverse matching is supported. The value can be **true** or **false**. The default value is **false**. This parameter is reserved.
key	String	Specifies the key of the match content. The default value is **null**. This parameter is reserved. The value contains a maximum of 255 characters.

Parameter	Type	Description
value	String	Specifies the value of the match content. The value contains a maximum of 128 characters. • When **type** is set to **HOST_NAME**, the value can contain a maximum of 100 characters that contain only letters, digits, hyphens (-), and periods (.), and must start with a letter or digit. • When **type** is set to **PATH**, the value can contain a maximum of 128 characters. When **compare_type** is set to **STARTS_WITH** or **EQUAL_TO**, the value must start with a slash (/) and can contain only letters, digits, and special characters _~';@^-%#&$.*+?,=!:| \/()[]{}
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the forwarding rule.

Example Request

- Example request: Adding a forwarding rule

```
POST https://{endpoint}/v2/a31d2bdcf7604c0faaddb058e1e08819/elb/l7policies/5ae0e1e7-5f0f-47a1-b39f-5d4c428a1586/rules

{
    "rule": {
        "compare_type": "EQUAL_TO",
        "type": "PATH",
        "value": "/bbb.html"
    }
}
```

Example Response

- Example response

```
{
    "rule": {
        "compare_type": "EQUAL_TO",
        "admin_state_up": true,
        "provisioning_status": "ACTIVE",
        "tenant_id": "a31d2bdcf7604c0faaddb058e1e08819",
        "project_id": "a31d2bdcf7604c0faaddb058e1e08819",
        "invert": false,
        "value": "/bbb.html",
        "key": null,
        "type": "PATH",
        "id": "c6f457b8-bf6f-45d7-be5c-a3226945b7b1"
    }
}
```


Status Code

For details, see **Status Codes**.

6.7.2 Querying Forwarding Rules

Function

This API is used to query forwarding rules. Filter query and pagination query are supported. Unless otherwise specified, exact match is applied.

Constraints

Parameters **marker**, **limit**, and **page_reverse** are used for pagination query. Parameters **marker** and **page_reverse** take effect only when they are used together with parameter **limit**.

URI

GET /v2/{project_id}/elb/l7policies/{l7policy_id}/rules

Table 6-177 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
l7policy_id	Yes	String	Specifies the forwarding policy ID.

Table 6-178 Query parameters

Parameter	Mandatory	Type	Description
marker	No	String	Specifies the ID of the forwarding rule from which pagination query starts, that is, the ID of the last forwarding rule on the previous page. This parameter must be used together with **limit**.
limit	No	Integer	Specifies the number of forwarding rules on each page. If this parameter is not set, all forwarding rules are queried by default.

Parameter	Mandatory	Type	Description
page_reverse	No	Boolean	Specifies the page direction. The value can be **true** or **false**, and the default value is **false**. The last page in the list requested with **page_reverse** set to **false** will not contain the "next" link, and the last page in the list requested with **page_reverse** set to **true** will not contain the "previous" link. This parameter must be used together with **limit**.
id	No	String	Specifies the forwarding rule ID.
tenant_id	No	String	Specifies the ID of the project where the forwarding rule is used. The value contains a maximum of 255 characters.
project_id	No	String	Specifies the ID of the project to which the forwarding rule belongs. This parameter has the same meaning as **tenant_id**.
admin_state_up	No	Boolean	Specifies the administrative status of the forwarding rule.
type	No	String	Specifies the match type of a forwarding rule. The value can be: • **HOST_NAME**: matches the domain name in the request. • **PATH**: matches the path in the request. The match type of forwarding rules in a forwarding policy must be unique.

Parameter	Mandatory	Type	Description
compare_type	No	String	Specifies the match mode. The options are as follows: When **type** is set to **HOST_NAME**, the value of this parameter can only be the following: • **EQUAL_TO**: indicates exact match. When **type** is set to **PATH**, the value of this parameter can be one of the following: • **REGEX**: indicates regular expression match. • **STARTS_WITH**: indicates prefix match. • **EQUAL_TO**: indicates exact match.
invert	No	Boolean	Specifies whether reverse matching is supported. The value can be **true** or **false**. The default value is **false**. This parameter is reserved.
key	No	String	Specifies the key of the match content. The default value is **null**. This parameter is reserved. The value contains a maximum of 255 characters.
value	No	String	Specifies the value of the match content. The value contains a maximum of 128 characters. • When **type** is set to **HOST_NAME**, the value can contain a maximum of 100 characters that contain only letters, digits, hyphens (-), and periods (.), and must start with a letter or digit. • When **type** is set to **PATH**, the value can contain a maximum of 128 characters. When **compare_type** is set to **STARTS_WITH** or **EQUAL_TO**, the value must start with a slash (/) and can contain only letters, digits, and special characters _~';@^-%#&$.*+?,=!:|\/()[]{}

Parameter	Mandatory	Type	Description
provisioning_status	No	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the forwarding rule.

Request

None

Response

Table 6-179 Parameter description

Parameter	Type	Description
rules	Array of **Rules** objects	Lists the forwarding rules. For details, see **Table 6-180**.

Table 6-180 rules parameter description

Parameter	Type	Description
id	String	Specifies the forwarding rule ID.
tenant_id	String	Specifies the ID of the project where the forwarding rule is used. The value contains a maximum of 255 characters.
project_id	String	Specifies the ID of the project to which the forwarding rule belongs. This parameter has the same meaning as **tenant_id**.
admin_state_up	Boolean	Specifies the administrative status of the forwarding rule. The value can only be **true**.
type	String	Specifies the match type of a forwarding rule. The value can be: • **HOST_NAME**: matches the domain name in the request. • **PATH**: matches the path in the request.

Parameter	Type	Description
compare_type	String	Specifies the match mode. The options are as follows: When **type** is set to **HOST_NAME**, the value of this parameter can only be the following: • **EQUAL_TO**: indicates exact match. When **type** is set to **PATH**, the value of this parameter can be one of the following: • **REGEX**: indicates regular expression match. • **STARTS_WITH**: indicates prefix match. • **EQUAL_TO**: indicates exact match.
invert	Boolean	Specifies whether reverse matching is supported. The value can be **true** or **false**. The default value is **false**. This parameter is reserved.
key	String	Specifies the key of the match content. The default value is **null**. This parameter is reserved. The value contains a maximum of 255 characters.
value	String	Specifies the value of the match content. The value contains a maximum of 128 characters. • When **type** is set to **HOST_NAME**, the value can contain a maximum of 100 characters that contain only letters, digits, hyphens (-), and periods (.), and must start with a letter or digit. • When **type** is set to **PATH**, the value can contain a maximum of 128 characters. When **compare_type** is set to **STARTS_WITH** or **EQUAL_TO**, the value must start with a slash (/) and can contain only letters, digits, and special characters _~';@^-%#&$.*+?,=!:| \/()[]{}
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the forwarding rule.

Example Request

- Example request: Querying all forwarding rules of a specific forwarding policy

```
GET https://{Endpoint}/v2/a31d2bdcf7604c0faaddb058e1e08819/elb/l7policies/5ae0e1e7-5f0f-47a1-b39f-5d4c428a1586/rules
```

Example Response

- Example response

```
{
   "rules": [
      {
         "compare_type": "EQUAL_TO",
         "provisioning_status": "ACTIVE",
         "admin_state_up": true,
         "tenant_id": "a31d2bdcf7604c0faaddb058e1e08819",
         "project_id": "a31d2bdcf7604c0faaddb058e1e08819",
         "invert": false,
         "value": "www.test.com",
         "key": null,
         "type": "HOST_NAME",
         "id": "67d8a8fa-b0dd-4bd4-a85b-671db19b2ef3"
      },
      {
         "compare_type": "EQUAL_TO",
         "provisioning_status": "ACTIVE",
         "admin_state_up": true,
         "tenant_id": "a31d2bdcf7604c0faaddb058e1e08819",
         "project_id": "a31d2bdcf7604c0faaddb058e1e08819",
         "invert": false,
         "value": "/aaa.html",
         "key": null,
         "type": "PATH",
         "id": "f02b3bca-69d2-4335-a3fa-a8054e996213"
      }
   ]
}
```

Status Code

For details, see **Status Codes**.

6.7.3 Querying Details of a Forwarding Rule

Function

This API is used to query details about a forwarding rule.

URI

GET /v2/{project_id}/elb/l7policies/{l7policy_id}/rules/{l7rule_id}

Table 6-181 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Parameter	Mandatory	Type	Description
l7policy_id	Yes	String	Specifies the forwarding policy ID.
l7rule_id	Yes	String	Specifies the forwarding rule ID.

Request

None

Response

Table 6-182 Parameter description

Parameter	Type	Description
rule	**Rule** object	Specifies the forwarding rule. For details, see **Table 6-183**.

Table 6-183 rule parameter description

Parameter	Type	Description
id	String	Specifies the forwarding rule ID.
tenant_id	String	Specifies the ID of the project where the forwarding rule is used. The value contains a maximum of 255 characters.
project_id	String	Specifies the ID of the project to which the forwarding rule belongs. This parameter has the same meaning as **tenant_id**.
admin_state_up	Boolean	Specifies the administrative status of the forwarding rule. The value can only be **true**.
type	String	Specifies the match type of a forwarding rule. The value can be: • **HOST_NAME**: matches the domain name in the request. • **PATH**: matches the path in the request.

Parameter	Type	Description
compare_type	String	Specifies the match mode. The options are as follows: When **type** is set to **HOST_NAME**, the value of this parameter can only be the following: • **EQUAL_TO**: indicates exact match. When **type** is set to **PATH**, the value of this parameter can be one of the following: • **REGEX**: indicates regular expression match. • **STARTS_WITH**: indicates prefix match. • **EQUAL_TO**: indicates exact match.
invert	Boolean	Specifies whether reverse matching is supported. The value can be **true** or **false**. The default value is **false**. This parameter is reserved.
key	String	Specifies the key of the match content. The default value is **null**. This parameter is reserved. The value contains a maximum of 255 characters.
value	String	Specifies the value of the match content. The value contains a maximum of 128 characters. • When **type** is set to **HOST_NAME**, the value can contain a maximum of 100 characters that contain only letters, digits, hyphens (-), and periods (.), and must start with a letter or digit. • When **type** is set to **PATH**, the value can contain a maximum of 128 characters. When **compare_type** is set to **STARTS_WITH** or **EQUAL_TO**, the value must start with a slash (/) and can contain only letters, digits, and special characters _~';@^-%#&$.*+?,=!:| \/()[]{}
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the forwarding rule.

Example Request

- Example request: Querying details of a forwarding rule
  GET https://{Endpoint}/v2/a31d2bdcf7604c0faaddb058e1e08819/elb/l7policies/5ae0e1e7-5f0f-47a1-b39f-5d4c428a1586/rules/67d8a8fa-b0dd-4bd4-a85b-671db19b2ef3

Example Response

- Example response 1

```
{
    "rule": {
        "compare_type": "EQUAL_TO",
        "provisioning_status": "ACTIVE",
        "admin_state_up": true,
        "tenant_id": "a31d2bdcf7604c0faaddb058e1e08819",
        "project_id": "a31d2bdcf7604c0faaddb058e1e08819",
        "invert": false,
        "value": "/index.html",
        "key": null,
        "type": "PATH",
        "id": "67d8a8fa-b0dd-4bd4-a85b-671db19b2ef3"
    }
}
```

Status Code

For details, see **Status Codes**.

6.7.4 Updating a Forwarding Rule

Function

This API is used to update a forwarding rule. You can change the mode that how traffic is distributed by updating the forwarding rule.

URI

PUT /v2/{project_id}/elb/l7policies/{l7policy_id}/rules/{l7rule_id}

Table 6-184 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
l7policy_id	Yes	String	Specifies the forwarding policy ID.
l7rule_id	Yes	String	Specifies the forwarding rule ID.

Request

Table 6-185 Parameter description

Parameter	Mandatory	Type	Description
rule	Yes	**Rule** object	Specifies the forwarding rule. For details, see **Table 6-186**.

Table 6-186 rule parameter description

Parameter	Mandatory	Type	Description
compare_type	No	String	Specifies the match mode. The options are as follows: When **type** is set to **HOST_NAME**, the value of this parameter can only be the following: • **EQUAL_TO**: indicates exact match. When **type** is set to **PATH**, the value of this parameter can be one of the following: • **REGEX**: indicates regular expression match. • **STARTS_WITH**: indicates prefix match. • **EQUAL_TO**: indicates exact match.
admin_state_up	No	Boolean	Specifies the administrative status of the forwarding rule. The value can only be **true**.
invert	No	Boolean	Specifies whether reverse matching is supported. The value can be **true** or **false**. The default value is **false**. This parameter is reserved.
key	No	String	Specifies the key of the match content. The default value is **null**. This parameter is reserved. The value contains a maximum of 255 characters.

Parameter	Mandatory	Type	Description
value	No	String	Specifies the value of the match content. The value cannot contain spaces. The value contains a maximum of 128 characters. • When **type** is set to **HOST_NAME**, the value can contain a maximum of 100 characters that contain only letters, digits, hyphens (-), and periods (.), and must start with a letter or digit. • When **type** is set to **PATH**, the value can contain a maximum of 128 characters. When **compare_type** is set to **STARTS_WITH** or **EQUAL_TO**, the value must start with a slash (/) and can contain only letters, digits, and special characters _~';@^-%#&$.* +?,=!:| \/()[]{}

Response

Table 6-187 Parameter description

Parameter	Type	Description
rule	**Rule** object	Specifies the forwarding rule. For details, see **Table 6-188**.

Table 6-188 rule parameter description

Parameter	Type	Description
id	String	Specifies the forwarding rule ID.
tenant_id	String	Specifies the ID of the project where the forwarding rule is used. The value contains a maximum of 255 characters.
project_id	String	Specifies the ID of the project to which the forwarding rule belongs. This parameter has the same meaning as **tenant_id**.
admin_state_up	Boolean	Specifies the administrative status of the forwarding rule. The value can only be **true**.

Parameter	Type	Description
type	String	Specifies the match type of a forwarding rule. The value can be: • **HOST_NAME**: matches the domain name in the request. • **PATH**: matches the path in the request.
compare_type	String	Specifies the match mode. The options are as follows: When **type** is set to **HOST_NAME**, the value of this parameter can only be the following: • **EQUAL_TO**: indicates exact match. When **type** is set to **PATH**, the value of this parameter can be one of the following: • **REGEX**: indicates regular expression match. • **STARTS_WITH**: indicates prefix match. • **EQUAL_TO**: indicates exact match.
invert	Boolean	Specifies whether reverse matching is supported. The value can be **true** or **false**. The default value is **false**. This parameter is reserved.
key	String	Specifies the key of the match content. The default value is **null**. This parameter is reserved. The value contains a maximum of 255 characters.
value	String	Specifies the value of the match content. The value contains a maximum of 128 characters. • When **type** is set to **HOST_NAME**, the value can contain a maximum of 100 characters that contain only letters, digits, hyphens (-), and periods (.), and must start with a letter or digit. • When **type** is set to **PATH**, the value can contain a maximum of 128 characters. When **compare_type** is set to **STARTS_WITH** or **EQUAL_TO**, the value must start with a slash (/) and can contain only letters, digits, and special characters _~';@^-%#&$.*+?,=!:| \/()[]{}

Parameter	Type	Description
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the forwarding rule.

Example Request

- Example request: Updating a forwarding rule

```
PUT https://{Endpoint}/v2/a31d2bdcf7604c0faaddb058e1e08819/elb/l7policies/5ae0e1e7-5f0f-47a1-b39f-5d4c428a1586/rules/c6f457b8-bf6f-45d7-be5c-a3226945b7b1

{
    "rule": {
        "compare_type": "STARTS_WITH",
        "value": "/ccc.html"
    }
}
```

Example Response

- Example response

```
{
    "rule": {
        "compare_type": "STARTS_WITH",
        "provisioning_status": "ACTIVE",
        "admin_state_up": true,
        "tenant_id": "a31d2bdcf7604c0faaddb058e1e08819",
        "project_id": "a31d2bdcf7604c0faaddb058e1e08819",
        "invert": false,
        "value": "/ccc.html",
        "key": null,
        "type": "PATH",
        "id": "c6f457b8-bf6f-45d7-be5c-a3226945b7b1"
    }
}
```

Status Code

For details, see **Status Codes**.

6.7.5 Deleting a Forwarding Rule

Function

This API is used to delete a forwarding rule.

URI

DELETE /v2/{project_id}/elb/l7policies/{l7policy_id}/rules/{l7rule_id}

Table 6-189 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
l7policy_id	Yes	String	Specifies the forwarding policy ID.
l7rule_id	Yes	String	Specifies the forwarding rule ID.

Request

None

Response

None

Example Request

- Example request: Deleting a forwarding rule
  ```
  DELETE https://{Endpoint}/v2/a31d2bdcf7604c0faaddb058e1e08819/elb/l7policies/5ae0e1e7-5f0f-47a1-b39f-5d4c428a1586/rules/c6f457b8-bf6f-45d7-be5c-a3226945b7b1
  ```

Example Response

- Example response

  None

Status Code

For details, see **Status Codes**.

6.8 Whitelist

6.8.1 Adding a Whitelist

Function

This API is used to add a whitelist to control access to a specific listener. After a whitelist is added, only IP addresses in the whitelist can access the listener.

URI

POST /v2/{project_id}/elb/whitelists

Table 6-190 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Request

Table 6-191 Parameter description

Parameter	Mandatory	Type	Description
whitelist	Yes	**Whitelist** object	Specifies the whitelist. For details, see **Table 6-192**.

Table 6-192 whitelist parameter description

Parameter	Mandatory	Type	Description
tenant_id	No	String	Specifies the ID of the project where the whitelist is used. The value must be the same as the value of **project_id** in the token. The value contains a maximum of 255 characters.
listener_id	Yes	String	Specifies the listener ID. Only one whitelist can be created for a listener.
enable_whitelist	No	Boolean	Specifies whether to enable access control. **true**: Access control is enabled. **false**: Access control is disabled. The default value is **true**.
whitelist	No	String	Specifies the IP addresses in the whitelist. Use commas (,) to separate multiple IP addresses. You can specify an IP address, for example, 192.168.11.1. You can also specify an IP address range, for example, 192.168.0.1/24. The default value is an empty string, that is, **""**.

Response

Table 6-193 Parameter description

Parameter	Type	Description
whitelist	**Whitelist** object	Specifies the whitelist. For details, see **Table 6-194**.

Table 6-194 whitelist parameter description

Parameter	Type	Description
id	String	Specifies the whitelist ID.
tenant_id	String	Specifies the ID of the project where the whitelist is used. The value contains a maximum of 255 characters.
listener_id	String	Specifies the ID of the listener to which the whitelist is added.
enable_whitelist	Boolean	Specifies whether to enable access control. **true**: Access control is enabled. **false**: Access control is disabled.
whitelist	String	Specifies the IP addresses in the whitelist.

Example Request

- Example request: Adding a whitelist

```
POST https://{Endpoint}/v2/eabfefa3fd1740a88a47ad98e132d238/elb/whitelists

{
    "whitelist": {
        "listener_id": "eabfefa3fd1740a88a47ad98e132d238",
        "enable_whitelist": true,
        "whitelist": "192.168.11.1,192.168.0.1/24,192.168.201.18/8,100.164.0.1/24"
    }
}
```

Example Response

- Example response

```
{
    "whitelist": {
        "id": "eabfefa3fd1740a88a47ad98e132d238",
        "listener_id": "eabfefa3fd1740a88a47ad98e132d238",
        "tenant_id": "eabfefa3fd1740a88a47ad98e132d238",
        "enable_whitelist": true,
        "whitelist": "192.168.11.1,192.168.0.1/24,192.168.201.18/8,100.164.0.1/24"
```



```
    }
}
```

Status Code

For details, see **Status Codes**.

6.8.2 Querying Details of a Whitelist

Function

This API is used to query details about a whitelist using its ID.

URI

GET /v2/{project_id}/elb/whitelists/{whitelist_id}

Table 6-195 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
whitelist_id	Yes	String	Specifies the whitelist ID.

Request

None

Response

Table 6-196 Parameter description

Parameter	Type	Description
whitelist	**Whitelist** object	Specifies the whitelist. For details, see **Table 6-197**.

Table 6-197 whitelist parameter description

Parameter	Type	Description
id	String	Specifies the whitelist ID.
tenant_id	String	Specifies the ID of the project where the whitelist is used. The value contains a maximum of 255 characters.

Parameter	Type	Description
listener_id	String	Specifies the ID of the listener to which the whitelist is added.
enable_whitelist	Boolean	Specifies whether to enable access control. **true**: Access control is enabled. **false**: Access control is disabled.
whitelist	String	Specifies the IP addresses in the whitelist.

Example Request

- Example request: Querying details of a whitelist
  ```
  GET https://{Endpoint}/v2/eabfefa3fd1740a88a47ad98e132d238/elb/whitelists/09e64049-2ab0-4763-a8c5-f4207875dc3e
  ```

Example Response

- Example response
  ```
  {
     "whitelist": {
        "id": "eabfefa3fd1740a88a47ad98e132d238",
        "listener_id": "eabfefa3fd1740a88a47ad98e132d238",
        "tenant_id": "eabfefa3fd1740a88a47ad98e132d238",
        "enable_whitelist": true,
        "whitelist": "192.168.11.1,192.168.0.1/24,192.168.201.18/8,100.164.0.1/24"
     }
  }
  ```

Status Code

For details, see **Status Codes**.

6.8.3 Querying Whitelists

Function

This API is used to query the whitelists. Filter query and pagination query are supported. Unless otherwise specified, exact match is applied.

Constraints

Parameters **marker**, **limit**, and **page_reverse** are used for pagination query. Parameters **marker** and **page_reverse** take effect only when they are used together with parameter **limit**.

URI

GET /v2/{project_id}/elb/whitelists

Table 6-198 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Table 6-199 Query parameters

Parameter	Mandatory	Type	Description
marker	No	String	Specifies the ID of the whitelist from which pagination query starts, that is, the ID of the last whitelist on the previous page. This parameter must be used together with **limit**.
limit	No	Integer	Specifies the number of whitelists on each page. If this parameter is not set, all whitelists are queried by default.
page_reverse	No	Boolean	Specifies the page direction. The value can be **true** or **false**, and the default value is **false**. The last page in the list requested with **page_reverse** set to **false** will not contain the "next" link, and the last page in the list requested with **page_reverse** set to **true** will not contain the "previous" link. This parameter must be used together with **limit**.
id	No	String	Specifies the whitelist ID.
tenant_id	No	String	Specifies the ID of the project where the whitelist is used. The value contains a maximum of 255 characters.
listener_id	No	String	Specifies the ID of the listener to which the whitelist is added.
enable_whitelist	No	Boolean	Specifies whether to enable access control. **true**: Access control is enabled. **false**: Access control is disabled.

Parameter	Mandatory	Type	Description
whitelist	No	String	Specifies the IP addresses in the whitelist.

Request

None

Response

Table 6-200 Parameter description

Parameter	Type	Description
whitelists	Array of **Whitelists** objects	Specifies the whitelist. For details, see **Table 6-201**.

Table 6-201 whitelists parameter description

Parameter	Type	Description
id	String	Specifies the whitelist ID.
tenant_id	String	Specifies the ID of the project where the whitelist is used. The value contains a maximum of 255 characters.
listener_id	String	Specifies the ID of the listener to which the whitelist is added.
enable_whitelist	Boolean	Specifies whether to enable access control. **true**: Access control is enabled. **false**: Access control is disabled.
whitelist	String	Specifies the IP addresses in the whitelist.

Example Request

- Example request 1: Querying all whitelists
  ```
  GET https://{Endpoint}/v2/eabfefa3fd1740a88a47ad98e132d238/elb/whitelists
  ```
- Example request 2: Querying the whitelists added to listener eabfefa3fd1740a88a47ad98e132d230


```
GET https://{Endpoint}/v2/eabfefa3fd1740a88a47ad98e132d238/elb/whitelists?
listener_id=eabfefa3fd1740a88a47ad98e132d230
```

Example Response

- Example response 1

```
{
   "whitelists": [
      {
         "id": "eabfefa3fd1740a88a47ad98e132d238",
         "listener_id": "eabfefa3fd1740a88a47ad98e132d238",
         "tenant_id": "eabfefa3fd1740a88a47ad98e132d238",
         "enable_whitelist": true,
         "whitelist": "192.168.11.1,192.168.0.1/24,192.168.201.18/8,100.164.0.1/24"
      },
      {
         "id": "eabfefa3fd1740a88a47ad98e132d326",
         "listener_id": "eabfefa3fd1740a88a47ad98e132d327",
         "tenant_id": "eabfefa3fd1740a88a47ad98e132d436",
         "enable_whitelist": true,
         "whitelist": "192.168.12.1,192.168.1.1/24,192.168.203.18/8,100.164.5.1/24"
      }
   ]
}
```

- Example response 2

```
{
   "whitelists": [
      {
         "id": "eabfefa3fd1740a88a47ad98e132d238",
         "listener_id": "eabfefa3fd1740a88a47ad98e132d230",
         "tenant_id": "eabfefa3fd1740a88a47ad98e132d239",
         "enable_whitelist": true,
         "whitelist": "192.168.11.1,192.168.0.1/24,192.168.201.18/8,100.164.0.1/24"
      },
      {
         "id": "eabfefa3fd1740a88a47ad98e132d326",
         "listener_id": "eabfefa3fd1740a88a47ad98e132d327",
         "tenant_id": "eabfefa3fd1740a88a47ad98e132d439",
         "enable_whitelist": true,
         "whitelist": "192.168.12.1,192.168.1.1/24,192.168.203.18/8,100.164.5.1/24"
      }
   ]
}
```

Status Code

For details, see **Status Codes**.

6.8.4 Updating a Whitelist

Function

This API is used to update a whitelist. You can enable or disable the whitelist function or change IP addresses in the whitelist. If you change IP addresses in the whitelist, it will be deleted, and a new one is generated.

URI

PUT /v2/{project_id}/elb/whitelists/{whitelist_id}

Table 6-202 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
whitelist_id	Yes	String	Specifies the whitelist ID.

Request

Table 6-203 Parameter description

Parameter	Mandatory	Type	Description
whitelist	Yes	**Whitelist** object	Specifies the whitelist. For details, see **Table 6-204**.

Table 6-204 whitelist parameter description

Parameter	Mandatory	Type	Description
enable_whitelist	No	Boolean	Specifies whether to enable access control. **true**: Access control is enabled. **false**: Access control is disabled. The default value is **true**.
whitelist	No	String	Specifies the IP addresses in the whitelist. Use commas (,) to separate multiple IP addresses. You can specify an IP address, for example, 192.168.11.1. You can also specify an IP address range, for example, 192.168.0.1/24. The default value is an empty string, that is, "".

Response

Table 6-205 Parameter description

Parameter	Type	Description
whitelist	**Whitelist** object	Specifies the whitelist. For details, see **Table 6-206**.

Table 6-206 whitelist parameter description

Parameter	Type	Description
id	String	Specifies the whitelist ID.
tenant_id	String	Specifies the ID of the project where the whitelist is used. The value contains a maximum of 255 characters.
listener_id	String	Specifies the ID of the listener to which the whitelist is added.
enable_whitelist	Boolean	Specifies whether to enable access control. **true**: Access control is enabled. **false**: Access control is disabled.
whitelist	String	Specifies the IP addresses in the whitelist.

Example Request

- Example request: Updating a whitelist

```
PUT https://{Endpoint}/v2/eabfefa3fd1740a88a47ad98e132d238/elb/whitelists/dcaf46f1-037c-4f63-a31f-e0c4c18032c7

{
    "whitelist": {
        "enable_whitelist": true,
        "whitelist": "192.168.11.1,192.168.0.1/24,192.168.201.18/8,100.164.0.1/24"
    }
}
```

Example Response

- Example response

```
{
    "whitelist": {
        "id": "eabfefa3fd1740a88a47ad98e132d238",
        "listener_id": "eabfefa3fd1740a88a47ad98e132d238",
        "tenant_id": "eabfefa3fd1740a88a47ad98e132d238",
        "enable_whitelist": true,
        "whitelist": "192.168.11.1,192.168.0.1/24,192.168.201.18/8,100.164.0.1/24"
```



```
  }
}
```

Status Code

For details, see **Status Codes**.

6.8.5 Deleting a Whitelist

Function

This API is used to delete a specific whitelist.

URI

DELETE /v2/{project_id}/elb/whitelists/{whitelist_id}

Table 6-207 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
whitelist_id	Yes	String	Specifies the whitelist ID.

Request

None

Response

None

Example Request

- Example request: Deleting a whitelist

```
DELETE https://{Endpoint}/v2/eabfefa3fd1740a88a47ad98e132d238/elb/whitelists/35cb8516-1173-4035-8dae-0dae3453f37f
```

Example Response

- Example response

  None

Status Code

For details, see **Status Codes**.

6.9 Certificate

6.9.1 Creating a Certificate

Function

This API is used to create a certificate. After a certificate is bound to a listener, the load balancer authenticates the client using this certificate, and backend servers can establish secure and reliable HTTP connections with the client.

URI

POST /v2/{project_id}/elb/certificates

Table 6-208 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Request

Table 6-209 Query parameters

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Specifies the administrative status of the certificate. This parameter is reserved, and the default value is **true**.
name	No	String	Specifies the certificate name. The value contains a maximum of 255 characters.
description	No	String	Provides supplementary information about the certificate. The value contains a maximum of 255 characters.

Parameter	Mandatory	Type	Description
type	No	String	Specifies the certificate type. The default value is **server**. The value can be: ● **server**: indicates the server certificate. ● **client**: indicates the CA certificate.
domain	No	String	Specifies the domain name associated with the server certificate. The default value is **null**. The value contains a maximum of 100 characters. Value range: ● A common domain name contains 0 to 100 characters and consists of several labels separated by periods (.). Each label can contain a maximum of 63 characters, including letters, digits, and hyphens (-), and must start and end with a letter or digit. ● In addition to the requirements for common domain names, a wildcard domain name can start with an asterisk (*). **NOTE** This parameter takes effect only when **type** is set to **server**.
private_key	No	String	Specifies the private key of the server certificate. The value must be PEM encoded. ● This parameter will be ignored if **type** is set to **client**. A CA server can still be created and used normally. This parameter will be left blank even if you enter a private key that is not PEM encoded. ● This parameter is mandatory only when **type** is set to **server**. If you enter an invalid private key, an error is returned.

Parameter	Mandatory	Type	Description
certificate	Yes	String	Specifies the public key of the server certificate or CA certificate used to authenticate the client. The value of parameter **type** determines whether a public key or CA certificate is required. Both types of certificates are in PEM format.
enterprise_project_id	No	String	Specifies the enterprise project ID. When creating a load balancer, you can assign an enterprise project to the load balancer. The value is character string **0** or a UUID with hyphens (-). Value **0** indicates the default enterprise project. The default value is **0**. **NOTE** For more information about enterprise projects and how to obtain enterprise project IDs, see **Enterprise Management User Guide**.
source	No	String	Specifies the source of the certificate. The default value is **null**. Constraints: If **scm_certificate_id** is not left blank and **source** is not specified, the default value is **scm**.
protection_status	No	String	Specifies the protection status. The value can be: • **nonProtection**: The load balancer is not protected. • **consoleProtection**: Modification protection is enabled to avoid that resources are modified by accident on the console. Default value: **nonProtection**
protection_reason	No	String	Specifies why the modification protection is enabled. **NOTE** This parameter is valid only when **protection_status** is set to **consoleProtection**.

Response

Table 6-210 Parameter description

Parameter	Type	Description
id	String	Specifies the certificate ID.
tenant_id	String	Specifies the ID of the project where the certificate is used. The value contains a maximum of 255 characters.
admin_state_up	Boolean	Specifies the administrative status of the certificate. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
name	String	Specifies the certificate name. The value contains a maximum of 255 characters.
description	String	Provides supplementary information about the certificate. The value contains a maximum of 255 characters.
type	String	Specifies the certificate type. The value can be: • **server**: indicates the server certificate. • **client**: indicates the CA certificate.
domain	String	Specifies the domain name associated with the server certificate. The value contains a maximum of 100 characters.
private_key	String	Specifies the private key of the server certificate in PEM format.
certificate	String	Specifies the public key of the server certificate or CA certificate used to authenticate the client. The value of parameter **type** determines whether a public key or CA certificate is required. Both types of certificates are in PEM format.
expire_time	String	Specifies the time when the certificate expires. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format.

Parameter	Type	Description
create_time	String	Specifies the time when the certificate was created. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format.
update_time	String	Specifies the time when the certificate was updated. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format.
source	String	Specifies the source of the certificate. The default value is **null**. Constraints: If **scm_certificate_id** is not left blank and **source** is not specified, the default value is **scm**.
protection_status	String	Specifies the protection status. The value can be: • **nonProtection**: The load balancer is not protected. • **consoleProtection**: Modification protection is enabled to avoid that resources are modified by accident on the console. Default value: **nonProtection**
protection_reason	String	Specifies why the modification protection is enabled.

Example Request

- Example request: Creating a certificate

```
POST https://{Endpoint}/v2/930600df07ac4f66964004041bd3deaf/elb/certificates
{
    "name": "https_certificate",
    "description": "description for certificate",
    "type": "server",
    "domain": "www.elb.com",
    "private_key":
"-----BEGIN PRIVATE KEY-----
\nMIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDQVAbOLe5xNf4M
\n253Wn9vhdUzojetjv4J+B7kYwsMhRcgdcJ8KCnX1nfzTvI2ksXlTQ2o9BkpStnPe
\ntB4s32ZiJRMlk+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM
\nMD30gLh6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8Icq39buNpIgDOWzEP5AzqXt
\nCOFYn6RTH5SRug4hKNN7sT1eYMslHu7wtEBDKVgrLjOCe/W2f8rLT1zEsoAW2Chl
\nZAPYUBkl/0XuTWRg3CohPPcI+UtlRSfvLDeeQ460swjbwgS/RbJh3sIwlCRLU08k
\nEo04Z9H/AgMBAAECggEAEIeaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/Hl
\nfvCArftGgMaYWPSNCJRMXB7tPwpQu19esjz4Z/cR2Je4fTLPrffGUsHFgZjv5OQB
\nZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr
\nciu9YkInNEHu6uRJ5g/eGGX3KQynTvVIhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M
\nEGpfYI6AdHIwFZcT/RNAxhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7Ale
\nkrguPtfV1vWklg+bUFhgGaiAEYTpAUN9t2DVIiijgQKBgQDnYMMsaF0r557CM1CT
\nXUqgCZo8MKeV2jf2drlxRRwRl33SksQbzAQ/qrLdT7GP3sCGqvkxWY2FPdFYf8kx
\nGcCeZPcIeZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/fbwjpjP7dt
\nJ7n8EzkRUNE6aIMHOFEeych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr
```


\niWgTWHXPZxUQaYhpjXo6+lMI6DpExiDgBAkMzJGIvS7yQiYWU+wthAr9urbWYdGZ
\nlS6VjoTkF6r7VZoILXX0fbuXh6lm8K8IQRfBpJff56p9phMwaBpDNDrfpHB5utBU
\nxs40yIdp6wKBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zJf3bGSXU/jR4eB
\n1lVQhELGI9CbKSdzKM71GyEImix/T7FnJSHIWlho1qVo6AQyduNWnAQD15pr8KAd
\nXGXAZZ1FQcb3KYa+2fflERmazdOTwjYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak
\n/735uP20KKqhNehZpC2dJei7OiIgRhCS/dKASUXHSW4fptBnUxACYocdDxtY4Vha
\nfI7FPMdvGl8ioYbvlHFh+X0Xs9r1S8yeWnHoXMb6eXWmYKMJrAoveLa+2cFm1Agf
\n7nLhA4R4lqm9IpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAJkD4wHW54Pwd4Ctfk9o
\njHjWB7pQlUYpTZO9dm+4fpCMn9Okf43AE2yAOaAP94GdzdDJkxfciXKcsYr9IIuk
\nfaoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BUlGKMWXzuEd
\n3fy+1rCUwzOp9LSjtJYf4ege\n-----END PRIVATE KEY-----",
"certificate":
"-----BEGIN CERTIFICATE-----
\nMIIC4TCCAcmgAwIBAgICEREwDQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXlD
\nb21wYW55IENBMB4XDTE4MDcwMjEzMjU0N1oXDTQ1MTExNzEzMjU0N1owFDESMBAG
\nA1UEAwwJbG9jYWxob3N0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
\n0FQGzi3ucTX+DNud1p/b4XVM6l3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5
\nU0NqPQZKUrZz3rQeLN9mYiUTJZPutYlFDDbB8CtlgV+eyU9yYJslWx/Bm5kWNPh9
\n7B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/W7jaS
\nIAzlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylYKy4zgnv1tn/K
\ny09cxLKAFtgoZWQD2FAZJf9F7k1kYNwqITz3CPlLZUUn7yw3nkOOtLMI28IEv0Wy
\nYd7CMJQkS1NPJBKNOGfR/wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29t
\nhwQKuUvJhwR/AAABMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCSqGSIb3DQEBCwUA
\nA4IBAQA8lMQJxaTey7EjXtRLSVlEAMftAQPG6jijNQuvIBQYUDauDT4W2XUZ5wAn
\njiOyQ83va672K1G9s8n6xlH+xwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDa
\nezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPRLYlzp1HMnI6hkjPk4PCZ
\nwKnha0dlScati9CCt3UzXSNJOSLalKdHErH08Iqd+1BchScxCfk0xNITn1HZZGmI
\n+vbmunok3A2lucI14rnsrcbkGYqxGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZ
\niYsGDVN+9QBd0eYUHce+77s96i3I\n-----END CERTIFICATE-----",
"source": "CCE",
"protection_status": "consoleProtection",
"protection_reason": "Note that the resource is created by the CCE. Modify the resource on the CCE portal. Otherwise, services may be interrupted."
}

Example Response

- Example response

{
"id": "61328fa3d4db432698e197b4927f91bf",
"tenant_id": "0c1503d710984bad92306faea3654dfd",
"admin_state_up": **true**,
"name": "https_certificate",
"description": "description for certificate",
"type": "server",
"domain": "www.elb.com",
"private_key": "-----BEGIN PRIVATE KEY-----
\nMIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDQVAbOLe5xNf4M
\n253Wn9vhdUzojetjv4J+B7kYwsMhRcgdcJ8KCnX1nfzTvI2ksXlTQ2o9BkpStnPe
\ntB4s32ZiJRMlk+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM
\nMD30gLh6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8Icq39buNpIgDOWzEP5AzqXt
\nCOFYn6RTH5SRug4hKNN7sT1eYMslHu7wtEBDKVgrLjOCe/W2f8rLT1zEsoAW2Chl
\nZAPYUBkl/0XuTWRg3CohPPcI+UtlRSfvLDeeQ460swjbwgS/RbJh3slwlCRLU08k
\nEo04Z9H/AgMBAAECggEAEIeaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/Hl
\nfvCArftGgMaYWPSNCJRMXB7tPwpQu19esjz4Z/cR2Je4fTLPrffGUsHFgZjv5OQB
\nZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr
\nciu9YkInNEHu6uRJ5g/eGGX3KQynTvVIhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M
\nEGpfYI6AdHIwFZcT/RNAxhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7Ale
\nkrguPtfV1vWklg+bUFhgGaiAEYTpAUN9t2DVIiijgQKBgQDnYMMsaF0r557CM1CT
\nXUqgCZo8MKeV2jf2drlxRRwRl33SksQbzAQ/qrLdT7GP3sCGqvkxWY2FPdFYf8kx
\nGcCeZPcIeZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/fbwjpjP7dt
\nJ7n8EzkRUNE6aIMHOFEeych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr
\niWgTWHXPZxUQaYhpjXo6+lMI6DpExiDgBAkMzJGIvS7yQiYWU+wthAr9urbWYdGZ
\nlS6VjoTkF6r7VZoILXX0fbuXh6lm8K8IQRfBpJff56p9phMwaBpDNDrfpHB5utBU
\nxs40yIdp6wKBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zJf3bGSXU/jR4eB
\n1lVQhELGI9CbKSdzKM71GyEImix/T7FnJSHIWlho1qVo6AQyduNWnAQD15pr8KAd
\nXGXAZZ1FQcb3KYa+2fflERmazdOTwjYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak
\n/735uP20KKqhNehZpC2dJei7OiIgRhCS/dKASUXHSW4fptBnUxACYocdDxtY4Vha
\nfI7FPMdvGl8ioYbvlHFh+X0Xs9r1S8yeWnHoXMb6eXWmYKMJrAoveLa+2cFm1Agf

\n7nLhA4R4lqm9IpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAJkD4wHW54Pwd4Ctfk9o
\njHjWB7pQlUYpTZO9dm+4fpCMn9Okf43AE2yAOaAP94GdzdDJkxfciXKcsYr9IIuk
\nfaoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BUlGKMWXzuEd
\n3fy+1rCUwzOp9LSjtJYf4ege
\n-----END PRIVATE KEY-----",
"certificate": "-----BEGIN CERTIFICATE-----
\nMIIC4TCCAcmgAwIBAgICEREwDQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXlD
\nb21wYW55IENBMB4XDTE4MDcwMjEzMjU0N1oXDTQ1MTExNzEzMjU0N1owFDESMBAG
\nA1UEAwwJbG9jYWxob3N0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
\n0FQGzi3ucTX+DNud1p/b4XVM6l3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5
\nU0NqPQZKUrZz3rQeLN9mYiUTJZPutYlFDDbB8CtlgV+eyU9yYJslWx/Bm5kWNPh9
\n7B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/W7jaS
\nIAzlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylYKy4zgnv1tn/K
\ny09cxLKAFtgoZWQD2FAZJf9F7k1kYNwqITz3CPlLZUUn7yw3nkOOtLMI28IEv0Wy
\nYd7CMJQkS1NPJBKNOGfR/wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29t
\nhwQKuUvJhwR/AAABMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCSqGSIb3DQEBCwUA
\nA4IBAQA8lMQJxaTey7EjXtRLSVlEAMftAQPG6jijNQuvIBQYUDauDT4W2XUZ5wAn
\njiOyQ83va672K1G9s8n6xlH+xwwdSNnozaKzC87vwSeZKlOdl9I5I98TGKI6OoDa
\nezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPRLYlzp1HMnI6hkjPk4PCZ
\nwKnha0dlScati9CCt3UzXSNJOSLalKdHErH08Iqd+1BchScxCfk0xNITn1HZZGmI
\n+vbmunok3A2lucI14rnsrcbkGYqxGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZ
\niYsGDVN+9QBd0eYUHce+77s96i3I
\n-----END CERTIFICATE-----",
"expire_time": "2026-09-24 07:45:00",
"create_time": "2024-10-30 08:36:50",
"update_time": "2024-10-30 08:36:50",
"source": "CCE",
"protection_status": "consoleProtection",
"protection_reason": "Note that the resource is created by the CCE. Modify the resource on the CCE portal. Otherwise, services may be interrupted."
}

Status Code

For details, see **Status Codes**.

6.9.2 Querying Certificates

Function

This API is used to query the certificates. Filter query and pagination query are supported. Unless otherwise specified, exact match is applied.

Constraints

Parameters **marker**, **limit**, and **page_reverse** are used for pagination query. Parameters **marker** and **page_reverse** take effect only when they are used together with parameter **limit**.

URI

GET /v2/{project_id}/elb/certificates

Table 6-211 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Table 6-212 Parameter description

Parameter	Mandatory	Type	Description
marker	No	String	Specifies the ID of the certificate from which pagination query starts, that is, the ID of the last certificate on the previous page. This parameter must be used together with **limit**.
limit	No	Integer	Specifies the number of certificates on each page. If this parameter is not set, all certificates are queried by default.
page_reverse	No	Boolean	Specifies the page direction. The value can be **true** or **false**, and the default value is **false**. The last page in the list requested with **page_reverse** set to **false** will not contain the "next" link, and the last page in the list requested with **page_reverse** set to **true** will not contain the "previous" link. This parameter must be used together with **limit**.
id	No	String	Specifies the certificate ID.
name	No	String	Specifies the certificate name. The value contains a maximum of 255 characters.
description	No	String	Provides supplementary information about the certificate. The value contains a maximum of 255 characters.
type	No	String	Specifies the certificate type. The default value is **server**. The value can be: • **server**: indicates the server certificate. • **client**: indicates the CA certificate.

Parameter	Mandatory	Type	Description
domain	No	String	Specifies the domain name associated with the server certificate. The default value is **null**. The value contains a maximum of 100 characters. Value range: ● A common domain name contains 0 to 100 characters and consists of several labels separated by periods (.). Each label can contain a maximum of 63 characters, including letters, digits, and hyphens (-), and must start and end with a letter or digit. ● In addition to the requirements for common domain names, a wildcard domain name can start with an asterisk (*). This parameter takes effect only when **type** is set to **server**.
private_key	No	String	Specifies the private key of the server certificate. The value must be PEM encoded. ● This parameter will be ignored if **type** is set to **client**. A CA server can still be created and used normally. This parameter will be left blank even if you enter a private key that is not PEM encoded. ● This parameter is mandatory only when **type** is set to **server**. If you enter an invalid private key, an error is returned.
certificate	No	String	Specifies the public key of the server certificate or CA certificate used to authenticate the client. The value of parameter **type** determines whether a public key or CA certificate is required. Both types of certificates are in PEM format.

Parameter	Mandatory	Type	Description
create_time	No	String	Specifies the time when the certificate was created. The UTC time is in *YYYY-MM-DD HH:MM:SS* format.
update_time	No	String	Specifies the time when the certificate was updated. The UTC time is in *YYYY-MM-DD HH:MM:SS* format.
source	No	String	Specifies the source of the certificate. The default value is **null**. Constraints: If **scm_certificate_id** is not left blank and **source** is not specified, the default value is **scm**.
protection_status	No	String	Specifies the protection status. The value can be: • **nonProtection**: The load balancer is not protected. • **consoleProtection**: Modification protection is enabled to avoid that resources are modified by accident on the console. Default value: **nonProtection**
protection_reason	No	String	Specifies why the modification protection is enabled. **NOTE** This parameter is valid only when **protection_status** is set to **consoleProtection**.

Request

None

Response

Table 6-213 Response parameters

Parameter	Type	Description
certificates	Array of **Certificates** objects	Lists the certificates. For details, see **Table 6-214**.
instance_num	Integer	Specifies the number of certificates.

Table 6-214 certificates parameter description

Parameter	Type	Description
id	String	Specifies the certificate ID.
tenant_id	String	Specifies the ID of the project where the certificate is used. The value contains a maximum of 255 characters.
admin_state_up	Boolean	Specifies the administrative status of the certificate. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
name	String	Specifies the certificate name. The value contains a maximum of 255 characters.
description	String	Provides supplementary information about the certificate. The value contains a maximum of 255 characters.
type	String	Specifies the certificate type. The value can be: • **server**: indicates the server certificate. • **client**: indicates the CA certificate.
domain	String	Specifies the domain name associated with the server certificate. The value contains a maximum of 100 characters.

Parameter	Type	Description
private_key	String	Specifies the private key of the server certificate in PEM format.
certificate	String	Specifies the public key of the server certificate or CA certificate used to authenticate the client. The value of parameter **type** determines whether a public key or CA certificate is required. Both types of certificates are in PEM format.
expire_time	String	Specifies the time when the certificate expires. The UTC time is in *YYYY-MM-DD HH:MM:SS* format.
create_time	String	Specifies the time when the certificate was created. The UTC time is in *YYYY-MM-DD HH:MM:SS* format.
update_time	String	Specifies the time when the certificate was updated. The UTC time is in *YYYY-MM-DD HH:MM:SS* format.
source	String	Specifies the source of the certificate. The default value is **null**. Constraints: If **scm_certificate_id** is not left blank and **source** is not specified, the default value is **scm**.
protection_status	String	Specifies the protection status. The value can be: • **nonProtection**: The load balancer is not protected. • **consoleProtection**: Modification protection is enabled to avoid that resources are modified by accident on the console. Default value: **nonProtection**
protection_reason	String	Specifies why the modification protection is enabled.

Example Request

- Request example 1: Querying all certificates
  ```
  GET https://{Endpoint}/v2/a31d2bdcf7604c0faaddb058e1e08819/elb/certificates
  ```
- Example 2: Querying a certificate whose ID is ef4d341365754a959556576501791b19 or ed40e8ea9957488ea82de025e35b74c0


```
GET https://{Endpoint}/v2/601240b9c5c94059b63d484c92cfe308/elb/certificates
?id=ef4d341365754a959556576501791b19&id=ed40e8ea9957488ea82de025e35b74c0
```

Example Response

- Example response 1

```
{
   "certificates": [
      {
         "certificate": "-----BEGIN CERTIFICATE-----
\nMIIC4TCCAcmgAwIBAgICEREwDQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXlD
\nb21wYW55IENBMB4XDTE4MDcwMjEzMjU0N1oXDTQ1MTExNzEzMjU0N1owFDESMBAG
\nA1UEAwwJbG9jYWxob3N0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA\n0FQGzi3ucTX
+DNud1p/
b4XVM6I3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5\nU0NqPQZKUrZz3rQeLN9mYiUTJZPutYlFDDb
B8CtlgV+eyU9yYJslWx/
Bm5kWNPh9\n7B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/W7jaS
\nIAzlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylYKy4zgnv1tn/K
\ny09cxLKAFtgoZWQD2FAZJf9F7k1kYNwqITz3CPlLZUUn7yw3nkOOtLMI28IEv0Wy
\nYd7CMJQkS1NPJBKNOGfR/wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29t
\nhwQKuUvJhwR/AAABMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCSqGSIb3DQEBCwUA
\nA4IBAQA8lMQJxaTey7EjXtRLSVlEAMftAQPG6jijNQuvIBQYUDauDT4W2XUZ5wAn
\njiOyQ83va672K1G9s8n6xlH+xwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDa
\nezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPRLYlzp1HMnI6hkjPk4PCZ
\nwKnha0dlScati9CCt3UzXSNJOSLalKdHErH08Iqd+1BchScxCfk0xNITn1HZZGmI\n
+vbmunok3A2lucI14rnsrcbkGYqxGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZ\niYsGDVN
+9QBd0eYUHce+77s96i3I\n-----END CERTIFICATE-----",
         "create_time": "2017-02-25 09:35:27",
         "expire_time": "2045-11-17 13:25:47",
         "description": "description for certificate",
         "domain": "www.elb.com",
         "id": "23ef9aad4ecb463580476d324a6c71af",
         "admin_state_up": true,
         "tenant_id": "a31d2bdcf7604c0faaddb058e1e08819",
         "name": "https_certificate",
         "private_key":
"-----BEGIN PRIVATE KEY-----
\nMIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDQVAbOLe5xNf4M
\n253Wn9vhdUzojetjv4J+B7kYwsMhRcgdcJ8KCnX1nfzTvI2ksXlTQ2o9BkpStnPe\ntB4s32ZiJRMlk
+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM
\nMD30gLh6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8Icq39buNpIgDOWzEP5AzqXt
\nCOFYn6RTH5SRug4hKNN7sT1eYMslHu7wtEBDKVgrLjOCe/W2f8rLT1zEsoAW2Chl\nZAPYUBkl/
0XuTWRg3CohPPcI+UtlRSfvLDeeQ460swjbwgS/RbJh3sIwlCRLU08k\nEo04Z9H/
AgMBAAECggEAEIeaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/Hl
\nfvCArftGgMaYWPSNCJRMXB7tPwpQu19esjz4Z/cR2Je4fTLPrffGUsHFgZjv5OQB
\nZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr
\nciu9YkInNEHu6uRJ5g/eGGX3KQynTvVIhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M\nEGpfYI6AdHIwFZcT/
RNAxhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7Ale\nkrguPtfV1vWklg
+bUFhgGaiAEYTpAUN9t2DVIiijgQKBgQDnYMMsaF0r557CM1CT
\nXUqgCZo8MKeV2jf2drlxRRwRl33SksQbzAQ/qrLdT7GP3sCGqvkxWY2FPdFYf8kx
\nGcCeZPcIeZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/fbwjpjP7dt
\nJ7n8EzkRUNE6aIMHOFEeych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr
\niWgTWHXPZxUQaYhpjXo6+lMI6DpExiDgBAkMzJGIvS7yQiYWU+wthAr9urbWYdGZ
\nlS6VjoTkF6r7VZoILXX0fbuXh6lm8K8IQRfBpJff56p9phMwaBpDNDrfpHB5utBU
\nxs40yIdp6wKBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zJf3bGSXU/jR4eB
\n1lVQhELGI9CbKSdzKM71GyEImix/T7FnJSHIWlho1qVo6AQyduNWnAQD15pr8KAd
\nXGXAZZ1FQcb3KYa+2fflERmazdOTwjYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak\n/
735uP20KKqhNehZpC2dJei7OiIgRhCS/dKASUXHSW4fptBnUxACYocdDxtY4Vha\nfI7FPMdvGl8ioYbvlHFh
+X0Xs9r1S8yeWnHoXMb6eXWmYKMJrAoveLa+2cFm1Agf
\n7nLhA4R4lqm9IpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAJkD4wHW54Pwd4Ctfk9o
\njHjWB7pQlUYpTZO9dm+4fpCMn9Okf43AE2yAOaAP94GdzdDJkxfciXKcsYr9IIuk
\nfaoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BUlGKMWXzuEd\n3fy
+1rCUwzOp9LSjtJYf4ege\n-----END PRIVATE KEY-----",
         "type": "server",
         "update_time": "2017-02-25 09:35:27",
         "source": "CCE",
         "protection_status": "consoleProtection",
         "protection_reason": "Note that the resource is created by the CCE. Modify the resource on
the CCE portal. Otherwise, services may be interrupted."
```



```
        }
    ],
    "instance_num": 1
}
```

- Example response 2

```
{
    "certificates": [
        {
            "description": "Push by SSL Certificate Manager",
            "domain": null,
            "id": "ed40e8ea9957488ea82de025e35b74c0",
            "name": "certForSonar9",
            "certificate": "-----BEGIN CERTIFICATE-----
MIIFizCCBHOgAwIBAgIQBlQycV3bWsVsCttvv5rgRjANBgkqhkiG9w0BAQsFADBu
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMS0wKwYDVQQDEyRFbmNyeXB0aW9uIEV2ZXJ5d2hlcmUg
RFYgVExTIENBIC0gRzEwHhcNMTgwNzEwMDAwMDAwWhcNMTkwNzEwMTIwMDAwWjAU
MRIwEAYDVQQDEwlpY2UxMjMudGswggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQCtTDlQMoAvyInR6X1dihhNwbdGesbMW6NZX7ffpj9XrB3KCqqlxzI4VmH9
PntvrpLJNeolgLqDZZc4zKbUkmqxY1dvGDs41coKzdtc9Ig23GVK48wfesnk5r50
afyU52R1JlSHDOhiDhHOSyhrOzc2GreLrByWKFUaAue6rTnyMbzQaSPtrTAqsURZ
wcmJ6R3A6JwokOgxXBSu41ufPQiFkMgxygKxEBLzIJLjRqCXQHYoxbsTyolb6jwp
w4H6vcRIEcFAgs98ApWRoEKjy7eOP3UUm05F+OkOvXhrlxEqIPm/rlwE0PmVlmm9
DgBafYb3xT/MtT2VRSfCJQHgIcsdAgMBAAGjggJ9MIICeTAfBgNVHSMEGDAWgBRV
dE+yck/1YLpQ0dfmUVyaAYca1zAdBgNVHQ4EFgQUEFavzYXBNbIHBchbaKcUKad+
qCEwIwYDVR0RBBwwGoIJaWNlMTIzLnRrgg13d3cuaWNlMTIzLnRrMA4GA1UdDwEB
/wQEAwIFoDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwTAYDVR0gBEUw
QzA3BglghkgBhv1sAQIwKjAoBggrBgEFBQcCARYcaHR0cHM6Ly93d3cuZGlnaWNl
cnQuY29tL0NQUzAIBgZngQwBAgEwgYEGCCsGAQUFBwEBBHUwczAlBggrBgEFBQcw
AYYZaHR0cDovL29jc3AyLmRpZ2ljZXJ0LmNvbTBKBggrBgEFBQcwAoY+aHR0cDov
L2NhY2VydHMuZGlnaWNlcnQuY29tL0VuY3J5cHRpb25FdmVyeXdoZXJlRFZUTFND
QS1HMS5jcnQwCQYDVR0TBAIwADCCAQQGCisGAQQB1nkCBAIEgfUEgfIA8AB2AKS5
CZC0GFgUh7sTosxncAo8NZgE+RvfuON3zQ7IDdwQAAABZIOnLCIAAAQDAEcwRQIh
AJX6gCXNggPdfOFdDtZPzlYr64TTrR/+b9QKKhyJ2EjBAiAWgu3BG2QK9tWQXpUN
IFadc0nvqmDovabg5nmRMan2mQB2AId1v+dZfPiMQ5lfvfNu/1aNR1Y2/0q1YMG0
6v9eoIMPAAABZIOnLQEAAAQDAEcwRQIhAJVRe/7n88dD6KdhNrd4LdFjGARQNmta
Y/K2dFDOXPSfAiBOLrWW8unHOL25RWHJU7Ost3XkNhQYtrLDJrnzo/9kZzANBgkq
hkiG9w0BAQsFAAOCAQEAeqtX9cHmj4OnNAk0IGmF3nKS/u/UgGsY4EJfXwQY2bTZ
PCkqxQOA6HEx59vJ+UilTojrNDi0WskRm/8SKBHtmRwzwX3ile8KiR6fFfQhPUtV
XHZcTfAFo47c7axqon8vumMlEv1PxVImivQ446K7z3kGm34dhMYxS4Gz2gTl8IKt
90OegejuhbAs5Wlvp1BK8HlYIb5+mw+cgkUC9KTALs5qVbWzogb0bS20KaYarGcu
otcZAOMeJdBFWnpzhr1fxmjaNY4u4hrgPZSTU/iBjdHapoza3zAFfxysmGYqs9dR
jFyxZeR4scz8GqSTFviNdH9jvtDJkdAC5hfMaB811Q==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEqjCCA5KgAwIBAgIQAnmsRYvBskWr+YBTzSybsTANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0xNzExMjcxMjQ2MTBaFw0yNzExMjcxMjQ2MTBaMG4xCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j
b20xLTArBgNVBAMTJEVuY3J5cHRpb24gRXZlcnl3aGVyZSBEViBUTFMgQ0EgLSBH
MTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALPeP6wkab41dyQh6mKc
oHqt3jRIxW5MDvf9QyiOR7VfFwK656es0UFiIb74N9pRntzF1UgYzDGu3ppZVMdo
lbxhm6dWS9OK/lFehKNT0OYI9aqk6F+U7cA6jxSC+iDBPXwdF4rs3KRyp3aQn6pj
pp1yr7IB6Y4zv72Ee/PlZ/6rK6InC6WpK0nPVOYR7n9iDuPe1E4IxUMBH/T33+3h
yuH3dvfgiWUOUkjdpMbyxX+XNle5uEIiyBsi4IvbcTCh8ruifCIi5mDXkZrnMT8n
wfYCV6v6kDdXkbgGRLKsR4pucbJtbKqIkUGxuZI2t7pfewKRc5nWecvDBZf3+p1M
pA8CAwEAAaOCAU8wggFLMB0GA1UdDgQWBBRVdE+yck/1YLpQ0dfmUVyaAYca1zAf
BgNVHSMEGDAWgBQD3lA1VtFMu2bwo+IbG8OXsj3RVTAOBgNVHQ8BAf8EBAMCAYYw
HQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMBIGA1UdEwEB/wQIMAYBAf8C
AQAwNAYIKwYBBQUHAQEEKDAmMCQGCCsGAQUFBzABhhhodHRwOi8vb2NzcC5kaWdp
Y2VydC5jb20wQgYDVR0fBDswOTA3oDWgM4YxaHR0cDovL2NybDMuZGlnaWNlcnQu
Y29tL0RpZ2lDZXJ0R2xvYmFsUm9vdENBLmNybDBMBgNVHSAERTBDMDcGCWCGSAGG
/WwBAjAqMCgGCCsGAQUFBwIBFhxodHRwczovL3d3dy5kaWdpY2VydC5jb20vQ1BT
MAgGBmeBDAECATANBgkqhkiG9w0BAQsFAAOCAQEAK3Gp6/aGq7aBZsxf/oQ+TD/B
SwW3AU4ETK+GQf2kFzYZkby5SFrHdPomunx2HBzViUchGoofGgg7gHW0W3MlQAXW
M0r5LUvStcr82QDWYNPaUy4taCQmyaJ+VB+6wxHstSigOlSNF2a6vg4rgexixeiV
4YSB03Yqp2t3TeZHM9ESfkus74nQyW7pRGezj+TC44xCagCQQOzzNmzEAP2SnCrJ
sNE2DpRVMnL8J6xBRdjmOsC3N6cQuKuRXbzByVBjCqAA8t1L0I+9wXJerLPyErjy
```



```
rMKWaBFLmfK/AHNF4ZihwPGOc7w6UHczBZXH5RFzJNnww+WnKuTPI0HfnVH8lg==
-----END CERTIFICATE-----",
            "type": "server",
            "create_time": "2019-03-03 16:32:30",
            "private_key": "-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEArUw5UDKAL8iJ0el9XYoYTcG3RnrGzFujWV+336Y/V6wdygqq
pccyOFZh/T57b66SyTXqJYC6g2WXOMym1JJqsWNXbxg7ONXKCs3bXPSINtxlSuPM
H3rJ5Oa+dGn8lOdkdSZUhwzoYg4Rzksoazs3Nhq3i6wclihVGgLnuq058jG80Gkj
7a0wKrFEWcHJiekdwOicKJDoMVwUruNbnz0IhZDIMcoCsRAS8yCS40agl0B2KMW7
E8qJW+o8KcOB+r3ESBHBQILPfAKVkaBCo8u3jj91FJtORfjpDr14a5cRKiD5v65c
BND5lZZpvQ4AWn2G98U/zLU9lUUnwiUB4CHLHQIDAQABAoIBAGs5rISompP2OwA8
virwVRVXdPUQ5oxvbuTPys+A59RxVIU8kFW+qJ4fJMYysOFrXLtOtq+5tK20YBru
1ZLVfVqAowrELXB/J2ID+WTMkLORLsNlq1kW+nC9LL6PDY98lLW/n7FoFSkGl5HT
AxFGNGUvpr2vIojuL6nGfmcM47uscJ9aP6IJxr4p70dhPVjZBdnMnXYwRkB3dZt/
E0B/p8J5i3oo5Rucv4DOfB+01wXGAVyx5/zce+NZdhyrivkj3hHV55SxGhVWzWhj
a3dAlbpKwYgfILj0inRdJYmIjBdbGb2HFix7+ncBg8B2oerJXC6/fANwRGu5/LZU
5xuPVWkCgYEA6an8TY1unIGLYL5aBJ16Tx4usqMyTXr/T4zkQyftRPMt+ZuxVQHl
GHsg7XvLFNd04MBZXtkZXaYVcpOm7OUYcl0i9ZAkWXXoXcBtn1Oom3gz/7RjAUnp
k+myvxCUSQ2JSz4u3QBtyPVyYNyBFXrKqdKfcYyG85+yQVHBNMVrdvMCgYEAvd0C
hFpm83ha+VQp+9XN1DYZNUyqhibj/E3X9jAn+gDbzlKxw/D9en2RIlQYUrl8+il8
QKk4cfOxJYStQfxptz8QBPVeLajDN67zJ0Rk8AB50HHHcNSU8uFkaO8KxsyVjbLS
+JltqfJAEraXLinbp1Fxcg9DsQdMd6cw2DmrWa8CgYEA1UjJOUzo80i4HYWDC4Vn
OEK3o22do+WqmEVlsfsG9BH5HEdGVe7V3EO/6aY+1/ZXBDPvH8mRAs9v8lbeXow7
hWClYZfB5jre8HyOU4l8dPUCmdxhJrL913rRIuASSqBlet32ztnuXCnWzp1X4nBj
/yF3UqFQKZ7SihcDAZVWo4sCgYEAj7al/BcNzIcynX2mldhdh583b4/Ll+YCNm2Z
5eDHscZKmx8fLcjRpZE8dXagPqXmwtj6E1vDvQWP9m06VDNCthFHB+nO0tLmidSk
evmbScuiaTRmmbJf2IThY0hlqNsc7PgKF2DTkIstEr0hLDFE8Z6FN6f0PiDfMcbd
Ax6L5EMCgYEA0+qhuQftKQkGdbXX9r3H8N0TVh27ByfL3kKVYy0dUJMvsOAq6d97
8mEhYhrYt88f1sFsPM7G09XpCcBXwiKxw8+CDt9auD4r1snBnILpqMPmanF4UDXH
L7s+4it+nIQy24P6g1PihtzsM+HD2UCErBiYUJdRK8Q9GGHdZojFk9Y=
-----END RSA PRIVATE KEY-----
",
            "update_time": "2019-03-03 16:32:30",
            "admin_state_up": true,
            "tenant_id": "601240b9c5c94059b63d484c92cfe308",
            "expire_time": "2019-07-10 12:00:00",
            "source": "CCE",
            "protection_status": "consoleProtection",
            "protection_reason": "Note that the resource is created by the CCE. Modify the resource on
the CCE portal. Otherwise, services may be interrupted."
        },
        {
            "description": null,
            "domain": "www.elb.com",
            "id": "ef4d341365754a959556576501791b19",
            "name": "certificate_28b824c8bbee419992fb7974b2911c72",
            "certificate": "-----BEGIN CERTIFICATE-----
MIIDpTCCAo2gAwIBAgIJAKdmmOBYnFvoMA0GCSqGSIb3DQEBCwUAMGkxCzAJBgNV
BAYTAnh4MQswCQYDVQQIDAJ4eDELMAkGA1UEBwwCeHgxCzAJBgNVBAoMAnh4MQsw
CQYDVQQLDAJ4eDELMAkGA1UEAwwCeHgxGTAXBgkqhkiG9w0BCQEWCnh4QDE2My5j
b20wHhcNMTcxMjA0MDM0MjQ5WhcNMjAxMjAzMDM0MjQ5WjBpMQswCQYDVQQGEwJ4
eDELMAkGA1UECAwCeHgxCzAJBgNVBAcMAnh4MQswCQYDVQQKDAJ4eDELMAkGA1UE
CwwCeHgxCzAJBgNVBAMMAnh4MRkwFwYJKoZIhvcNAQkBFgp4eEAxNjMuY29tMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwZ5UJULAjWr7p6FVwGRQRjFN
2s8tZ/6LC3X82fajpVsYqF1xqEuUDndDXVD09E4u83MS6HO6a3bIVQDp6/klnYld
iE6Vp8HH5BSKaCWKVg8lGWg1UM9wZFnlryi14KgmpIFmcu9nA8yV/6MZAe6RSDmb
3iyNBmiZ8aZhGw2pI1YwR+15MVqFFGB+7ExkziROi7L8CFCyCezK2/oOOvQsH1dz
Q8z1JXWdg8/9Zx7Ktvgwu5PQM3cJtSHX6iBPOkMU8Z8TugLlTqQXKZOEgwajwvQ5
mf2DPkVgM08XAgaLJcLigwD513koAdtJd5v+9irw+5LAuO3JclqwTvwy7u/YwwID
AQABo1AwTjAdBgNVHQ4EFgQUo5A2tIu+bcUfvGTD7wmEkhXKFjcwHwYDVR0jBBgw
FoAUo5A2tIu+bcUfvGTD7wmEkhXKFjcwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0B
AQsFAAOCAQEAWJ2rS6Mvlqk3GfEpboezx2J3X7l1z8Sxoqg6ntwB+rezvK3mc9H0
83qcVeUcoH+0A0lSHyFN4FvRQL6X1hEheHarYwJK4agb231vb5erasuGO463eYEG
r4SfTuOm7SyiV2xxbaBKrXJtpBp4WLL/s+LF+nklKjaOxkmxUX0sM4CTA7uFJypY
c8Tdr8lDDNqoUtMD8BrUCJi+7lmMXRcC3Qi3oZJW76ja+kZA5mKVFPd1ATih8TbA
i34R7EQDtFeiSvBdeKRsPp8c0KT8H1B4lXNkkCQs2WX5p4lm99+ZtLD4glw8x6Ic
i1YhgnQbn5E0hz55OLu5jvOkKQjPCW+8Kg==
-----END CERTIFICATE-----",
            "type": "server",
```

```
            "create_time": "2018-09-28 03:00:47",
            "private_key": "-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAwZ5UJULAjWr7p6FVwGRQRjFN2s8tZ/6LC3X82fajpVsYqF1x
qEuUDndDXVD09E4u83MS6HO6a3bIVQDp6/klnYldiE6Vp8HH5BSKaCWKVg8lGWg1
UM9wZFnlryi14KgmpIFmcu9nA8yV/6MZAe6RSDmb3iyNBmiZ8aZhGw2pI1YwR+15
MVqFFGB+7ExkziROi7L8CFCyCezK2/oOOvQsH1dzQ8z1JXWdg8/9Zx7Ktvgwu5PQ
M3cJtSHX6iBPOkMU8Z8TugLlTqQXKZOEgwajwvQ5mf2DPkVgM08XAgaLJcLigwD5
13koAdtJd5v+9irw+5LAuO3JclqwTvwy7u/YwwIDAQABAoIBACU9S5fjD9/jTMXA
DRs08A+gGgZUxLn0xk+NAPX3LyB1tfdkCaFB8BccLzO6h3KZuwQOBPv6jkdvEDbx
Nwyw3eA/9GJsIvKiHc0rejdvyPymaw9I8MA7NbXHaJrY7KpqDQyk6sx+aUTcy5jg
iMXLWdwXYHhJ/1HVOo603oZyiS6HZeYU089NDUcX+1SJi3e5Ke0gPVXEqCq1O11/
rh24bMxnwZo4PKBWdcMBN5Zf/4ij9vrZE+fFzW7vGBO48A5lvZxWU2U5t/OZQRtN
1uLOHmMFa0FIF2aWbTVfwdUWAFsvAOkHj9VV8BXOUwKOUuEktdkfAlvrxmsFrO/H
yDeYYPkCgYEA/S55CBbR0sMXpSZ56uRn8JHApZJhgkgvYr+FqDlJq/e92nAzf01P
RoEBUajwrnf1ycevN/SDfbtWzq2XJGqhWdJmtpO16b7KBsC6BdRcH6dnOYh31jgA
vABMIP3wzI4zSVTyxRE8LDuboytF1mSCeV5tHYPQTZNwrplDnLQhywcCgYEAw8Yc
Uk/eiFr3hfH/ZohMfV5p82Qp7DNIGRzw8YtVG/3+vNXrAXW1VhugNhQY6L+zLtJC
aKn84ooup0m3YCg0hvINqJuvzfsuzQgtjTXyaE0cEwsjUusOmiuj09vVx/3U7siK
Hdjd2ICPCvQ6Q8tdi8jV320gMs05AtaBkZdsiWUCgYEAtLw4Kk4f+xTKDFsrLUNf
75wcqhWVBiwBp7yQ7UX4EYsJPKZcHMRTk0EEcAbpyaJZE3I44vjp5ReXIHNLMfPs
uvI34J4Rfot0LN3n7cFrAi2+wpNo+MOBwrNzpRmijGP2uKKrq4JiMjFbKV/6utGF
Up7VxfwS904JYpqGaZctiIECgYA1A6nZtF0riY6ry/uAdXpZHL8ONNqRZtWoT0kD
79otSVu5ISiSiRbaGcXsDExC52oKrSDAgFtbqQUiEOFg09UcXfoR6HwRkba2CiDwve
yHQLQI5Qrdxz8Mk0gIrNrSM4FAmcW9vi9z4kCbQyoC5C+4gqeUlRpDIkQBWP2Y4
2ct/bQKBgHv8qCsQTZphOxc31BJPa2xVhuv18cEU3XLUrVfUZ/1f43JhLp7gynS2
ep++LKUi9D0VGXY8bqvfJjbECoCeu85vl8NpCXwe/LoVoIn+7KaVIZMwqoGMfgNl
nEqm7HWkNxHhf8A6En/IjleuddS1sf9e/x+TJN1Xhnt9W6pe7Fk1
-----END RSA PRIVATE KEY-----",
            "update_time": "2018-09-28 03:00:47",
            "admin_state_up": true,
            "tenant_id": "601240b9c5c94059b63d484c92cfe308",
            "expire_time": "2020-12-03 03:42:49",
            "source": "CCE",
            "protection_status": "consoleProtection",
            "protection_reason": "Note that the resource is created by the CCE. Modify the resource on the CCE portal. Otherwise, services may be interrupted."
        }
    ],
    "instance_num": 2
}
```


Status Code

For details, see **Status Codes**.

6.9.3 Querying Details of a Certificate

Function

This API is used to query details about a certificate.

Constraints

None

URI

GET /v2/{project_id}/elb/certificates/{certificate_id}

Table 6-215 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
certificate_id	Yes	String	Specifies the certificate ID.

Request

None

Response

Table 6-216 Parameter description

Parameter	Type	Description
id	String	Specifies the certificate ID.
tenant_id	String	Specifies the ID of the project where the certificate is used. The value contains a maximum of 255 characters.
admin_state_up	Boolean	Specifies the administrative status of the certificate. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
name	String	Specifies the certificate name. The value contains a maximum of 255 characters.
description	String	Provides supplementary information about the certificate. The value contains a maximum of 255 characters.
type	String	Specifies the certificate type. The value can be: • **server**: indicates the server certificate. • **client**: indicates the CA certificate.

Parameter	Type	Description
domain	String	Specifies the domain name associated with the server certificate. The value contains a maximum of 100 characters.
private_key	String	Specifies the private key of the server certificate in PEM format.
certificate	String	Specifies the public key of the server certificate or CA certificate used to authenticate the client. The value of parameter **type** determines whether a public key or CA certificate is required. Both types of certificates are in PEM format.
expire_time	String	Specifies the time when the certificate expires. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format.
create_time	String	Specifies the time when the certificate was created. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format.
update_time	String	Specifies the time when the certificate was updated. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format.
source	String	Specifies the source of the certificate. The default value is **null**. Constraints: If **scm_certificate_id** is not left blank and **source** is not specified, the default value is **scm**.
protection_status	String	Specifies the protection status. The value can be: • **nonProtection**: The load balancer is not protected. • **consoleProtection**: Modification protection is enabled to avoid that resources are modified by accident on the console. Default value: **nonProtection**
protection_reason	String	Specifies why the modification protection is enabled.

Example Request

- Example request: Querying details of a certificate

```
GET https://{Endpoint}/v2/a31d2bdcf7604c0faaddb058e1e08819/elb/certificates/
23ef9aad4ecb463580476d324a6c71af
```

Example Response

- Example response 1


```
{
    "certificate":
"-----BEGIN CERTIFICATE-----
\nMIIC4TCCAcmgAwIBAgICEREwDQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXlD
\nb21wYW55IENBMB4XDTE4MDcwMjEzMjU0N1oXDTQ1MTExNzEzMjU0N1owFDESMBAG
\nA1UEAwwJbG9jYWxob3N0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
\n0FQGzi3ucTX+DNud1p/b4XVM6l3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5
\nU0NqPQZKUrZz3rQeLN9mYiUTJZPutYlFDDbB8CtlgV+eyU9yYJslWx/Bm5kWNPh9
\n7B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/W7jaS
\nIAzlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylYKy4zgnv1tn/K
\ny09cxLKAFtgoZWQD2FAZJf9F7k1kYNwqITz3CPlLZUUn7yw3nkOOtLMI28IEv0Wy
\nYd7CMJQkS1NPJBKNOGfR/wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29t
\nhwQKuUvJhwR/AAABMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCSqGSIb3DQEBCwUA
\nA4IBAQA8lMQJxaTey7EjXtRLSVlEAMftAQPG6jijNQuvIBQYUDauDT4W2XUZ5wAn
\njiOyQ83va672K1G9s8n6xlH+xwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDa
\nezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPRLYlzp1HMnI6hkjPk4PCZ
\nwKnha0dlScati9CCt3UzXSNJOSLalKdHErH08Iqd+1BchScxCfk0xNITn1HZZGmI
\n+vbmunok3A2lucI14rnsrcbkGYqxGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZ
\niYsGDVN+9QBd0eYUHce+77s96i3I
\n-----END CERTIFICATE-----",
    "create_time": "2017-02-25 09:35:27",
    "expire_time": "2045-11-17 13:25:47",
    "description": "description for certificate",
    "domain": "www.elb.com",
    "id": "23ef9aad4ecb463580476d324a6c71af",
    "tenant_id": "a31d2bdcf7604c0faaddb058e1e08819",
    "admin_state_up": true,
    "name": "https_certificate",
    "private_key":
"-----BEGIN PRIVATE KEY-----
\nMIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDQVAbOLe5xNf4M
\n253Wn9vhdUzojetjv4J+B7kYwsMhRcgdcJ8KCnX1nfzTvI2ksXlTQ2o9BkpStnPe
\ntB4s32ZiJRMlk+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM
\nMD30gLh6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8Icq39buNpIgDOWzEP5AzqXt
\nCOFYn6RTH5SRug4hKNN7sT1eYMslHu7wtEBDKVgrLjOCe/W2f8rLT1zEsoAW2Chl
\nZAPYUBkl/0XuTWRg3CohPPcI+UtlRSfvLDeeQ460swjbwgS/RbJh3slwlCRLU08k
\nEo04Z9H/AgMBAAECggEAEIeaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/Hl
\nfvCArftGgMaYWPSNCJRMXB7tPwpQu19esjz4Z/cR2Je4fTLPrffGUsHFgZjv5OQB
\nZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr
\nciu9YkInNEHu6uRJ5g/eGGX3KQynTvVIhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M
\nEGpfYI6AdHIwFZcT/RNAxhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7Ale
\nkrguPtfV1vWklg+bUFhgGaiAEYTpAUN9t2DVIiijgQKBgQDnYMMsaF0r557CM1CT
\nXUqgCZo8MKeV2jf2drlxRRwRl33SksQbzAQ/qrLdT7GP3sCGqvkxWY2FPdFYf8kx
\nGcCeZPcIeZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/fbwjpjP7dt
\nJ7n8EzkRUNE6aIMHOFEeych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr
\niWgTWHXPZxUQaYhpjXo6+lMI6DpExiDgBAkMzJGIvS7yQiYWU+wthAr9urbWYdGZ
\nlS6VjoTkF6r7VZoILXX0fbuXh6lm8K8IQRfBpJff56p9phMwaBpDNDrfpHB5utBU
\nxxs40yIdp6wKBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zJf3bGSXU/jR4eB
\n1lVQhELGI9CbKSdzKM71GyEImix/T7FnJSHIWlho1qVo6AQyduNWnAQD15pr8KAd
\nXGXAZZ1FQcb3KYa+2fflERmazdOTwjYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak
\n/735uP20KKqhNehZpC2dJei7OiIgRhCS/dKASUXHSW4fptBnUxACYocdDxtY4Vha
\nfI7FPMdvGl8ioYbvlHFh+X0Xs9r1S8yeWnHoXMb6eXWmYKMJrAoveLa+2cFm1Agf
\n7nLhA4R4lqm9IpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAJkD4wHW54Pwd4Ctfk9o
\njHjWB7pQlUYpTZO9dm+4fpCMn9Okf43AE2yAOaAP94GdzdDJkxfciXKcsYr9IIuk
\nfaoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BUlGKMWXzuEd
\n3fy+1rCUwzOp9LSjtJYf4ege
\n-----END PRIVATE KEY-----",
    "type": "server",
    "update_time": "2017-02-25 09:35:27",
    "source": "CCE",
```



```
    "protection_status": "consoleProtection",
    "protection_reason": "Note that the resource is created by the CCE. Modify the resource on the CCE portal. Otherwise, services may be interrupted."
}
```


Status Code

For details, see **Status Codes**.

6.9.4 Updating a Certificate

Function

This API is used to update a certificate.

URI

PUT /v2/{project_id}/elb/certificates/{certificate_id}

Table 6-217 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
certificate_id	Yes	String	Specifies the certificate ID.

Request

Table 6-218 Parameter description

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Specifies the administrative status of the certificate. This parameter is reserved, and the default value is **true**.
name	No	String	Specifies the certificate name. The value contains a maximum of 255 characters.
description	No	String	Provides supplementary information about the certificate. The value contains a maximum of 255 characters.

Parameter	Mandatory	Type	Description
domain	No	String	Specifies the domain name associated with the server certificate. The default value is **null**. The value contains a maximum of 100 characters. Value range: • A common domain name contains 0 to 100 characters and consists of several labels separated by periods (.). Each label can contain a maximum of 63 characters, including letters, digits, and hyphens (-), and must start and end with a letter or digit. • In addition to the requirements for common domain names, a wildcard domain name can start with an asterisk (*). This parameter takes effect only when **type** is set to **server**. **NOTE** This parameter takes effect only when **type** is set to **server**.
private_key	No	String	Specifies the private key of the server certificate. The value must be PEM encoded. • This parameter will be ignored if **type** is set to **client**. A CA server can still be created and used normally. This parameter will be left blank even if you enter a private key that is not PEM encoded. • This parameter is mandatory only when **type** is set to **server**. If you enter an invalid private key, an error is returned.
certificate	No	String	Specifies the public key of the server certificate or CA certificate used to authenticate the client. The value of parameter **type** determines whether a public key or CA certificate is required. Both types of certificates are in PEM format.

Parameter	Mandatory	Type	Description
source	No	String	Specifies the source of the certificate. The default value is **null**. Constraints: If **scm_certificate_id** is not left blank and **source** is not specified, the default value is **scm**.
protection_status	No	String	Specifies the protection status. The value can be: • **nonProtection**: The load balancer is not protected. • **consoleProtection**: Modification protection is enabled to avoid that resources are modified by accident on the console. Default value: **nonProtection**
protection_reason	No	String	Specifies why the modification protection is enabled. **NOTE** This parameter is valid only when **protection_status** is set to **consoleProtection**.

Response

Table 6-219 Parameter description

Parameter	Type	Description
id	String	Specifies the certificate ID.
tenant_id	String	Specifies the ID of the project where the certificate is used. The value contains a maximum of 255 characters.
admin_state_up	Boolean	Specifies the administrative status of the certificate. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
name	String	Specifies the certificate name. The value contains a maximum of 255 characters.

Parameter	Type	Description
description	String	Provides supplementary information about the certificate. The value contains a maximum of 255 characters.
type	String	Specifies the certificate type. The value can be: • **server**: indicates the server certificate. • **client**: indicates the CA certificate.
domain	String	Specifies the domain name associated with the server certificate. The value contains a maximum of 100 characters.
private_key	String	Specifies the private key of the server certificate in PEM format.
certificate	String	Specifies the public key of the server certificate or CA certificate used to authenticate the client. The value of parameter **type** determines whether a public key or CA certificate is required. Both types of certificates are in PEM format.
expire_time	String	Specifies the time when the certificate expires. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format.
create_time	String	Specifies the time when the certificate was created. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format.
update_time	String	Specifies the time when the certificate was updated. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format.
source	String	Specifies the source of the certificate. The default value is **null**. Constraints: If **scm_certificate_id** is not left blank and **source** is not specified, the default value is **scm**.

Parameter	Type	Description
protection_status	String	Specifies the protection status. The value can be: • **nonProtection**: The load balancer is not protected. • **consoleProtection**: Modification protection is enabled to avoid that resources are modified by accident on the console. Default value: **nonProtection**
protection_reason	String	Specifies why the modification protection is enabled.

Example Request

- Example request: Updating a certificate

```
PUT https://{Endpoint}/v2/a31d2bdcf7604c0faaddb058e1e08819/elb/certificates/
23ef9aad4ecb463580476d324a6c71af

{
   "certificate":
"-----BEGIN CERTIFICATE-----
\nMIIC4TCCAcmgAwIBAgICEREwDQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXlD
\nb21wYW55IENBMB4XDTE4MDcwMjEzMjU0N1oXDTQ1MTExNzEzMjU0N1owFDESMBAG
\nA1UEAwwJbG9jYWxob3N0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
\n0FQGzi3ucTX+DNud1p/b4XVM6I3rY7+Cfge5GMLDIUXlHXCfCgp19Z3807yNpLF5
\nU0NqPQZKUrZz3rQeLN9mYiUTJZPutYlFDDbB8CtlgV+eyU9yYJslWx/Bm5kWNPh9
\n7B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/W7jaS
\nIAzlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylYKy4zgnv1tn/K
\ny09cxLKAFtgoZWQD2FAZJf9F7k1kYNwqITz3CPlLZUUn7yw3nkOOtLMI28IEv0Wy
\nYd7CMJQkS1NPJBKNOGfR/wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29t
\nhwQKuUvJhwR/AAABMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCSqGSIb3DQEBCwUA
\nA4IBAQA8lMQJxaTey7EjXtRLSVlEAMftAQPG6jijNQuvIBQYUDauDT4W2XUZ5wAn
\njiOyQ83va672K1G9s8n6xlH+xwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDa
\nezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPRLYlzp1HMnI6hkjPk4PCZ
\nwKnha0dlScati9CCt3UzXSNJOSLalKdHErH08Iqd+1BchScxCfk0xNITn1HZZGmI
\n+vbmunok3A2lucI14rnsrcbkGYqxGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZ
\niYsGDVN+9QBd0eYUHce+77s96i3I
\n-----END CERTIFICATE-----",
   "description": "description for certificate",
   "domain": "www.elb.com",
   "name": "https_certificate",
   "private_key":
"-----BEGIN PRIVATE KEY-----
\nMIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDQVAbOLe5xNf4M
\n253Wn9vhdUzojetjv4J+B7kYwsMhRcgdcJ8KCnX1nfzTvI2ksXlTQ2o9BkpStnPe
\ntB4s32ZiJRMlk+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM
\nMD30gLh6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8Icq39buNpIgDOWzEP5AzqXt
\nCOFYn6RTH5SRug4hKNN7sT1eYMslHu7wtEBDKVgrLjOCe/W2f8rLT1zEsoAW2Chl
\nZAPYUBkl/0XuTWRg3CohPPcI+UtlRSfvLDeeQ460swjbwgS/RbJh3slwlCRLU08k
\nEo04Z9H/AgMBAAECggEAEIeaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/Hl
\nfvCArftGgMaYWPSNCJRMXB7tPwpQu19esjz4Z/cR2Je4fTLPrffGUsHFgZjv5OQB
\nZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr
\nciu9YkInNEHu6uRJ5g/eGGX3KQynTvVIhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M
\nEGpfYI6AdHIwFZcT/RNAxhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7Ale
\nkrguPtfV1vWklg+bUFhgGaiAEYTpAUN9t2DVIiijgQKBgQDnYMMsaF0r557CM1CT
\nXUqgCZo8MKeV2jf2drlxRRwRl33SksQbzAQ/qrLdT7GP3sCGqvkxWY2FPdFYf8kx
\nGcCeZPcIeZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/fbwjpjP7dt
\nJ7n8EzkRUNE6aIMHOFEeych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr
\niWgTWHXPZxUQaYhpjXo6+lMI6DpExiDgBAkMzJGIvS7yQiYWU+wthAr9urbWYdGZ
```

```
\nlS6VjoTkF6r7VZoILXX0fbuXh6lm8K8IQRfBpJff56p9phMwaBpDNDrfpHB5utBU
\nxs40yIdp6wKBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zJf3bGSXU/jR4eB
\n1lVQhELGI9CbKSdzKM71GyEImix/T7FnJSHIWlho1qVo6AQyduNWnAQD15pr8KAd
\nXGXAZZ1FQcb3KYa+2fflERmazdOTwjYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak
\n/735uP20KKqhNehZpC2dJei7OiIgRhCS/dKASUXHSW4fptBnUxACYocdDxtY4Vha
\nfI7FPMdvGl8ioYbvlHFh+X0Xs9r1S8yeWnHoXMb6eXWmYKMJrAoveLa+2cFm1Agf
\n7nLhA4R4lqm9IpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAJkD4wHW54Pwd4Ctfk9o
\njHjWB7pQlUYpTZO9dm+4fpCMn9Okf43AE2yAOaAP94GdzdDJkxfciXKcsYr9IIuk
\nfaoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BUlGKMWXzuEd
\n3fy+1rCUwzOp9LSjtJYf4ege
\n-----END PRIVATE KEY-----"
}
```

Example Response

- Example response 1

```
{
    "certificate": "-----BEGIN CERTIFICATE-----
\nMIIC4TCCAcmgAwIBAgICEREwDQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXlD
\nb21wYW55IENBMB4XDTE4MDcwMjEzMjU0N1oXDTQ1MTExNzEzMjU0N1owFDESMBAG
\nA1UEAwwJbG9jYWxob3N0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA\n0FQGzi3ucTX
+DNud1p/
b4XVM6I3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5\nU0NqPQZKUrZz3rQeLN9mYiUTJZPutYlFDDb
B8CtlgV+eyU9yYJslWx/
Bm5kWNPh9\n7B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/W7jaS
\nIAzlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylYKy4zgnv1tn/K
\ny09cxLKAFtgoZWQD2FAZJf9F7k1kYNwqITz3CPlLZUUn7yw3nkOOtLMI28IEv0Wy
\nYd7CMJQkS1NPJBKNOGfR/wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29t
\nhwQKuUvJhwR/AAABMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCSqGSIb3DQEBCwUA
\nA4IBAQA8lMQJxaTey7EjXtRLSVlEAMftAQPG6jijNQuvIBQYUDauDT4W2XUZ5wAn
\njiOyQ83va672K1G9s8n6xlH+xwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDa
\nezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPRLYlzp1HMnI6hkjPk4PCZ
\nwKnha0dlScati9CCt3UzXSNJOSLalKdHErH08Iqd+1BchScxCfk0xNITn1HZZGmI\n
+vbmunok3A2lucI14rnsrcbkGYqxGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZ\niYsGDVN
+9QBd0eYUHce+77s96i3I\n-----END CERTIFICATE-----",
    "expire_time": "2045-11-17 13:25:47",
    "create_time": "2017-02-25 09:35:27",
    "update_time": "2017-02-25 09:38:27",
    "id": "23ef9aad4ecb463580476d324a6c71af",
    "description": "description for certificate",
    "domain": "www.elb.com",
    "type": "server",
    "admin_state_up": true,
    "tenant_id": "a31d2bdcf7604c0faaddb058e1e08819",
    "name": "https_certificate",
    "private_key": "-----BEGIN PRIVATE KEY-----
\nMIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDQVAbOLe5xNf4M
\n253Wn9vhdUzojetjv4J+B7kYwsMhRcgdcJ8KCnX1nfzTvI2ksXlTQ2o9BkpStnPe\ntB4s32ZiJRMlk
+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM
\nMD30gLh6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8Icq39buNpIgDOWzEP5AzqXt
\nCOFYn6RTH5SRug4hKNN7sT1eYMslHu7wtEBDKVgrLjOCe/W2f8rLT1zEsoAW2Chl\nZAPYUBkl/
0XuTWRg3CohPPcl+UtlRSfvLDeeQ460swjbwgS/RbJh3slwlCRLU08k\nEo04Z9H/
AgMBAAECggEAEIeaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/Hl
\nfvCArftGgMaYWPSNCJRMXB7tPwpQu19esjz4Z/cR2Je4fTLPrffGUsHFgZjv5OQB
\nZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr
\nciu9YkInNEHu6uRJ5g/eGGX3KQynTvVIhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M\nEGpfYI6AdHIwFZcT/
RNAxhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7Ale\nkrguPtfV1vWklg
+bUFhgGaiAEYTpAUN9t2DVIiijgQKBgQDnYMMsaF0r557CM1CT
\nXUqgCZo8MKeV2jf2drlxRRwRl33SksQbzAQ/qrLdT7GP3sCGqvkxWY2FPdFYf8kx
\nGcCeZPcIeZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/fbwjpjP7dt
\nJ7n8EzkRUNE6aIMHOFEeych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr
\niWgTWHXPZxUQaYhpjXo6+lMI6DpExiDgBAkMzJGIvS7yQiYWU+wthAr9urbWYdGZ
\nlS6VjoTkF6r7VZoILXX0fbuXh6lm8K8IQRfBpJff56p9phMwaBpDNDrfpHB5utBU
\nxs40yIdp6wKBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zJf3bGSXU/jR4eB
\n1lVQhELGI9CbKSdzKM71GyEImix/T7FnJSHIWlho1qVo6AQyduNWnAQD15pr8KAd
\nXGXAZZ1FQcb3KYa+2fflERmazdOTwjYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak\n/
735uP20KKqhNehZpC2dJei7OiIgRhCS/dKASUXHSW4fptBnUxACYocdDxtY4Vha\nfI7FPMdvGl8ioYbvlHFh
+X0Xs9r1S8yeWnHoXMb6eXWmYKMJrAoveLa+2cFm1Agf
\n7nLhA4R4lqm9IpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAJkD4wHW54Pwd4Ctfk9o
```



```
\njHjWB7pQlUYpTZO9dm+4fpCMn9Okf43AE2yAOaAP94GdzdDJkxfciXKcsYr9IIuk
\nfaoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BUlGKMWXzuEd\n3fy
+1rCUwzOp9LSjtJYf4ege\n-----END PRIVATE KEY-----"
}
```

Status Code

For details, see **Status Codes**.

6.9.5 Deleting a Certificate

Function

This API is used to delete a certificate.

Constraints

If the target certificate is used by a listener, the certificate cannot be deleted, and 409 code will be displayed.

URI

DELETE /v2/{project_id}/elb/certificates/{certificate_id}

Table 6-220 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.
certificate_id	Yes	String	Specifies the certificate ID.

Request

None

Response

None

Example Request

- Example request: Deleting a certificate

```
DELETE https://{Endpoint}/v2/a31d2bdcf7604c0faaddb058e1e08819/elb/certificates/
23ef9aad4ecb463580476d324a6c71af
```

Example Response

- Example response

  None

Status Code

For details, see **Status Codes**.

7 APIs (OpenStack)

7.1 Tag

7.1.1 Adding a Tag to a Load Balancer

Function

This API is used to add a tag to a specific load balancer for easier management.

Constraints

A maximum of 20 tags can be added to a load balancer.

Note the following when you add tags:

- If there are duplicate keys in the request body, an error is reported.
- If there are no duplicate keys in the request body but the key in the request body exists in the database, the key in the database is overwritten.

URI

POST /v2.0/{project_id}/loadbalancers/{loadbalancer_id}/tags

Table 7-1 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the ID of the project where the tag is used.
loadbalancer_id	Yes	String	Specifies the ID of the load balancer to which a tag is to be added.

Request Parameters

Table 7-2 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token

Table 7-3 Parameter description

Parameter	Mandatory	Type	Description
tag	Yes	Object	Specifies the tag. For details, see **Table 7-4**.

Table 7-4 tag parameter description

Parameter	Mandatory	Type	Description
key	Yes	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 load balancer must be unique.
value	Yes	String	Specifies the tag value. • Can contain a maximum of 255 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-).

Response Parameters

None

Example Request

- Example request

```
POST https://{Endpoint}/v2.0/6a0de1c3-7d74-4f4a-b75e-e57135bd2b97/loadbalancers/7add33ad-11dc-4ab9-a50f-419703f13163/tags

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



```
  }
}
```

Example Response

- Example response

  None

Status Code

For details, see **Status Codes**.

7.1.2 Batch Adding Load Balancer Tags

Function

This API is used to batch add tags to a load balancer.

Constraints

A maximum of 20 tags can be added to a listener.

This API is idempotent.

- Note the following when you add tags:
  - If there are duplicate keys in the request body, an error is reported.
  - If there are no duplicate keys in the request body but the key in the request body exists in the database, the key in the database is overwritten.
  - The value of **action** must be **create**.

URI

POST /v2.0/{project_id}/loadbalancers/{loadbalancer_id}/tags/action

Table 7-5 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the ID of the project where the tag is used.
loadbalancer_id	Yes	String	Specifies the ID of the load balancer to which a tag is to be added.

Request Parameters

Table 7-6 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token

Table 7-7 Parameter description

Parameter	Mandatory	Type	Description
tags	Yes	Array	Lists the tags. For details, see **Table 7-8**.
action	Yes	String	Specifies the operation type. The value can be one of the following: • **create**: adds tags to the load balancer.

Table 7-8 tags parameter description

Parameter	Mandatory	Type	Description
key	Yes	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 load balancer must be unique.
value	Yes	String	Specifies the tag value. • Can contain a maximum of 255 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-).

Response Parameters

None

Example Request

- Example request

```
POST https://{Endpoint}/v2.0/6a0de1c3-7d74-4f4a-b75e-e57135bd2b97/loadbalancers/7add33ad-11dc-4ab9-a50f-419703f13163/tags/action

{
   "action": "create",
   "tags": [
      {
         "key": "key1",
         "value": "value1"
      },
      {
         "key": "key2",
         "value": "value2"
      }
   ]
}
```

Example Response

- Example response

  None

Status Code

For details, see **Status Codes**.

7.1.3 Batch Deleting Load Balancer Tags

Function

This API is used to batch delete tags from a load balancer.

Constraints

A maximum of 20 tags can be added to a listener.

This API is idempotent.

- Note the following when you delete the tags:
  - If the tag does not exist, the deletion is considered successful by default.
  - The value range of the tag character set is not verified.
  - The tag structure body cannot be missing, and the key cannot be left blank or set to an empty string.
  - The value of **action** must be **delete**.

URI

POST /v2.0/{project_id}/loadbalancers/{loadbalancer_id}/tags/action

Table 7-9 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the ID of the project where the tag is used.
loadbalancer_id	Yes	String	Specifies the ID of the load balancer from which a tag is to be deleted.

Request Parameters

Table 7-10 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the user token.

Table 7-11 Request parameters

Parameter	Mandatory	Type	Description
tags	Yes	Array	Specifies the tags. For details, see **Table 7-12**.
action	Yes	String	Specifies the operation type. The value can be: • **delete**: deletes tags from the load balancer.

Table 7-12 Parameter description

Parameter	Mandatory	Type	Description
key	Yes	String	Specifies the tag name. The tag: • Cannot be left blank. • Can contain a maximum of 128 characters. • Can contain letters, digits, underscores (_), and hyphens (-). • Cannot have the same key with other tags added to the same load balancer.
value	Yes	String	Specifies the tag value. The value: • Can contain a maximum of 255 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-).

Response Parameters

None

Example Request

- Example request

```
POST https://{Endpoint}/v2.0/6a0de1c3-7d74-4f4a-b75e-e57135bd2b97/loadbalancers/7add33ad-11dc-4ab9-a50f-419703f13163/tags/action

{
    "action": "delete",
    "tags": [
        {
            "key": "key1",
            "value": "value1"
        },
        {
            "key": "key2",
            "value": "value2"
        }
    ]
}
```

Example Response

- Example response

  None

Status Code

For details, see **Status Codes**.

7.1.4 Querying All Tags of a Load Balancer

Function

This API is used to query all the tags of one load balancer.

URI

GET /v2.0/{project_id}/loadbalancers/{loadbalancer_id}/tags

Table 7-13 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the ID of the project where the tag is used.
loadbalancer_id	Yes	String	Specifies the ID of the load balancer whose tags are to be queried.

Request Parameters

Table 7-14 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token

Response Parameters

Table 7-15 Response parameters

Parameter	Type	Description
tags	Array	Lists the tags. For details, see **Table 7-16**.

Table 7-16 tags parameter description

Parameter	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 load balancer 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 Request

- Example request
  ```
  GET https://{Endpoint}/v2.0/6a0de1c3-7d74-4f4a-b75e-e57135bd2b97/loadbalancers/7add33ad-11dc-4ab9-a50f-419703f13163/tags
  ```

Example Response

- Example response
  ```
  {
     "tags": [
        {
           "key": "key1",
           "value": "value1"
        },
        {
           "key": "key2",
           "value": "value2"
        }
     ]
  }
  ```

Status Code

For details, see **Status Codes**.

7.1.5 Querying the Tags of All Load Balancers

Function

This API is used to query the tags of all the load balancers.

URI

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

Table 7-17 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the ID of the project where the tag is used.

Request Parameters

Table 7-18 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token

Response Parameters

Table 7-19 Response parameters

Parameter	Type	Description
tags	Array	Lists the tags. For details, see **Table 7-20**.

Table 7-20 tags parameter description

Parameter	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 load balancer must be unique.
values	Array	Lists the tag values. • Can contain a maximum of 255 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-).

Example Request

- Example request
  GET https://{Endpoint}/v2.0/6a0de1c3-7d74-4f4a-b75e-e57135bd2b97/loadbalancers/tags

Example Response

- Example response

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

Status Code

For details, see **Status Codes**.

7.1.6 Querying Load Balancers by Tag

Function

This API is used to query load balancers using tags.

Constraints

None

URI

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

Table 7-21 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the ID of the project where the tag is used.

Request Parameters

Table 7-22 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token

Table 7-23 Parameter description

Parameter	Mandatory	Type	Description
tags	No	Array	Specifies the included tags. A maximum of 20 keys are allowed for each query operation, and each key can have a maximum of 20 values. The tag key cannot be left blank or set to an empty string. Each tag key and each tag value of the same tag key must be unique. For details, see **Table 7-24**.
limit	No	Integer	Sets the page size. This parameter is available when **action** is set to **filter**. Both the default value and maximum value are **1000**, and the minimum value is **1**. The value cannot be a negative integer.
offset	No	Integer	Specifies the index position. The query starts from the next load balancer indexed by this parameter. This parameter is not required when you query load balancers on the first page. The value in the response returned for querying the load balancers on the previous page will be included in this parameter for querying the load balancers 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 positive integer, and the default value is **0**.
action	Yes	String	Identifies the operation. The value can be **filter** or **count**. **filter**: indicates pagination query. **count**: indicates that all load balancers meeting the search criteria will be returned.

Parameter	Mandatory	Type	Description
matches	No	Array	Specifies the search criteria. The tag key is the parameter to match, for example, **resource_name**. **value** indicates the value of the match content. The key is a fixed dictionary value. For details, see **Table 7-25**.

Table 7-24 tags parameter description

Parameter	Mandatory	Type	Description
key	Yes	String	Specifies the tag key. It contains a maximum of 128 Unicode characters and cannot be left blank. (This parameter is not verified in the search process.)
values	Yes	Array	Lists the tag values. Each tag value can contain a maximum of 255 Unicode characters. The values are in the OR relationship. If no tag values in the list, the tag key is used for full search. If each value in the list starts with an asterisk (*), fuzzy match is performed based on the part after the asterisk.

Table 7-25 matches parameter description

Parameter	Mandatory	Type	Description
key	Yes	String	Specifies the tag key for match. The value can be one of the following: • **resource_name**: indicates the resource name. • **resource_id**: indicates the resource ID.
value	Yes	String	Specifies the tag value for match. Each tag value can contain a maximum of 255 Unicode characters.

Response Parameters

Table 7-26 Response parameters

Parameter	Type	Description
resources	Array	Lists the load balancers. For details, see **Table 7-27**.
total_count	Integer	Specifies the total number of queried records.

Table 7-27 resource parameter description

Parameter	Type	Description
resource_id	String	Specifies the resource ID.
resource_detail	String	Specifies the resource details. The value is a resource object, used for extension. The value is left blank by default.
tags	Array	Lists the tags. If there is no tag, an empty array is used by default. For details, see **Table 7-28**.
resource_name	String	Specifies the resource name. This parameter is an empty string by default if there is no resource name.
super_resource_id	String	Specifies the parent resource ID.

Table 7-28 tags parameter description

Parameter	Type	Description
key	String	Specifies the tag key. It contains a maximum of 128 Unicode characters and cannot be left blank. (This parameter is not verified in the search process.)
value	String	Specifies the tag value. Each tag value can contain a maximum of 255 Unicode characters.

Example Request

- Example request 1 (when **action** is set to **filter**)
  ```
  POST https://{Endpoint}/v2.0/6a0de1c3-7d74-4f4a-b75e-e57135bd2b97/loadbalancers/resource_instances/action
  ```



```
{
   "offset": "100",
   "limit": "100",
   "action": "filter",
   "matches": [
      {
         "key": "resource_name",
         "value": "resource1"
      }
   ],
   "tags": [
      {
         "key": "key1",
         "values": [
            "*value1",
            "value2"
         ]
      }
   ]
}
```

- Example request 2 (when **action** is set to **count**)

```
POST https://{Endpoint}/v2.0/6a0de1c3-7d74-4f4a-b75e-e57135bd2b97/loadbalancers/
resource_instances/action

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

Example Response

- Example response 1

```
{
   "resources": [
      {
         "resource_detail": "",
         "resource_id": "154d135b-3a89-4e89-8023-06efb9acdc05",
         "resource_name": "resouece1",
         "tags": [
            {
               "key": "key1",
               "value": "value1"
            },
            {
               "key": "key2",
               "value": "value1"
```



```
            }
          ]
        }
    ],
    "total_count": 1000
}
```

- Example response 2

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

Status Code

For details, see **Status Codes**.

7.1.7 Deleting a Tag from a Load Balancer

Function

This API is used to delete a tag with a specific key from a load balancer.

Constraints

None

URI

DELETE /v2.0/{project_id}/loadbalancers/{loadbalancer_id}/tags/{key}

Table 7-29 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the ID of the project where the tag is used.
loadbalancer_id	Yes	String	Specifies the ID of the load balancer from which a tag is to be deleted.

Request Parameters

Table 7-30 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token

Response Parameters

None

Example Request

- Example request
  DELETE https://{Endpoint}/v2.0/6a0de1c3-7d74-4f4a-b75e-e57135bd2b97/loadbalancers/7add33ad-11dc-4ab9-a50f-419703f13163/tags/key1

Example Response

- Example response
  None

Status Code

For details, see **Status Codes**.

7.1.8 Adding a Tag to a Listener

Function

This API is used to add a tag to a specific listener.

Constraints

- A maximum of 20 tags can be added to a load balancer.
- Note the following when you add tags:
  - If there are duplicate keys in the request body, an error is reported.
  - If there are no duplicate keys in the request body but the key in the request body exists in the database, the key in the database is overwritten.

URI

POST /v2.0/{project_id}/listeners/{listener_id}/tags

Table 7-31 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the ID of the project where the tag is used.
listener_id	Yes	String	Specifies the ID of the listener to which a tag is to be added.

Request Parameters

Table 7-32 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token

Table 7-33 Parameter description

Parameter	Mandatory	Type	Description
tag	Yes	Object	Specifies the tag. For details, see **Table 7-34**.

Table 7-34 tag parameter description

Parameter	Mandatory	Type	Description
key	Yes	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 listener must be unique.
value	Yes	String	Specifies the tag value. • Can contain a maximum of 255 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-).

Response Parameters

None

Example Request

- Example request

```
POST https://{Endpoint}/v2.0/6a0de1c3-7d74-4f4a-b75e-e57135bd2b97/listeners/7add33ad-11dc-4ab9-a50f-419703f13163/tags

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

Example Response

- Example response

  None

Status Code

For details, see **Status Codes**.

7.1.9 Batch Adding Tags to a Listener

Function

This API is used to batch add tags to a listener.

Constraints

- A maximum of 20 tags can be added to a listener.
- This API is idempotent.
- Note the following when you add tags:
  - If there are duplicate keys in the request body, an error is reported.
  - If there are no duplicate keys in the request body but the key in the request body exists in the database, the key in the database is overwritten.
  - The value of **action** must be **create**.

URI

POST /v2.0/{project_id}/listeners/{listener_id}/tags/action

Table 7-35 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the ID of the project where the tag is used.
listener_id	Yes	String	Specifies the ID of the listener to which tags are to be added.

Request Parameters

Table 7-36 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token

Table 7-37 Parameter description

Parameter	Mandatory	Type	Description
tags	Yes	Array	Lists the tags. For details, see **Table 7-38**.
action	Yes	String	Specifies the operation identifier. The value can be one of the following: • **create**: adds tags to the listener.

Table 7-38 resource_tag parameter description

Parameter	Mandatory	Type	Description
key	Yes	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 listener must be unique.
value	Yes	String	Specifies the tag value. • Can contain a maximum of 255 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-).

Response Parameters

None

Example Request

- Example request

```
POST https://{Endpoint}/v2.0/6a0de1c3-7d74-4f4a-b75e-e57135bd2b97/listeners/7add33ad-11dc-4ab9-a50f-419703f13163/tags/action

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



```
    {
        "key": "key1",
        "value": "value1"
    },
    {
        "key": "key2",
        "value": "value2"
    }
  ]
}
```

Example Response

- Example response

  None

Status Code

For details, see **Status Codes**.

7.1.10 Batch Deleting Tags from a Listener

Function

This API is used to batch delete tags from a listener.

Constraints

- A maximum of 20 tags can be added to a listener.
- This API is idempotent.
- Note the following when you delete tags:
  - If the tag to be deleted does not exist, the deletion is considered successful by default.
  - The value range of the tag character set is not verified.
  - The tag structure body cannot be missing, and the key cannot be left blank or set to an empty string.
  - The value of **action** must be **delete**.

URI

POST /v2.0/{project_id}/listeners/{listener_id}/tags/action

Table 7-39 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the ID of the project where the tag is used.
listener_id	Yes	String	Specifies the ID of the listener from which a tag is to be deleted.

Request Parameters

Table 7-40 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the user token.

Table 7-41 Request parameters

Parameter	Mandatory	Type	Description
tags	Yes	Array	Specifies the tags. For details, see **Table 7-42**.
action	Yes	String	Specifies the operation identifier. The value can be: • **delete**: deletes tags from the load balancer.

Table 7-42 resource_tag parameter description

Parameter	Mandatory	Type	Description
key	Yes	String	Specifies the tag name. The tag: • Cannot be left blank. • Can contain a maximum of 128 characters. • Can contain letters, digits, underscores (_), and hyphens (-). • Cannot have the same key with other tags added to the same load balancer.
value	Yes	String	Specifies the tag value. The value: • Can contain a maximum of 255 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-).

Response Parameters

None

Example Request

- Example request

```
POST https://{Endpoint}/v2.0/6a0de1c3-7d74-4f4a-b75e-e57135bd2b97/listeners/7add33ad-11dc-4ab9-a50f-419703f13163/tags/action

{
   "action": "delete",
   "tags": [
      {
         "key": "key1",
         "value": "value1"
      },
      {
         "key": "key2",
         "value": "value2"
      }
   ]
}
```

Example Response

- Example response

  None

Status Code

For details, see **Status Codes**.

7.1.11 Querying All Tags of a Listener

Function

This API is used to query all tags of one listener.

Constraints

None

URI

GET /v2.0/{project_id}/listeners/{listener_id}/tags

Table 7-43 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the ID of the project where the tag is used.

Parameter	Mandatory	Type	Description
listener_id	Yes	String	Specifies the ID of the listener whose tags are to be queried.

Request Parameters

Table 7-44 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token

Response Parameters

Table 7-45 Response parameters

Parameter	Type	Description
tags	Array	Lists the tags. For details, see **Table 7-46**.

Table 7-46 tags parameter description

Parameter	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 listener 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 Request

- Example request
  GET https://{Endpoint}/v2.0/6a0de1c3-7d74-4f4a-b75e-e57135bd2b97/listeners/7add33ad-11dc-4ab9-a50f-419703f13163/tags

Example Response

- Example response

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

Status Code

For details, see **Status Codes**.

7.1.12 Querying the Tags of All Listeners

Function

This API is used to query the tags of all listeners.

Constraints

None

URI

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

Table 7-47 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the ID of the project where the tag is used.

Request Parameters

Table 7-48 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token

Response Parameters

Table 7-49 Response parameters

Parameter	Type	Description
tags	Array	Lists the tags, which are aggregated by the tag key. For details, see **Table 7-50**. For example, if you have two listeners, the tag key of both listeners is "test", the tag value of listener A is "value1", and the tag value of listener B is "value2", two tags are queried, the key of both tags is "test", and the tag values are ["value1","value2"].

Table 7-50 tags parameter description

Parameter	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 listener must be unique.
values	Array	Lists the tag values. • Can contain a maximum of 255 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-).

Example Request

- Example request
  GET https://{Endpoint}/v2.0/6a0de1c3-7d74-4f4a-b75e-e57135bd2b97/listeners/tags

Example Response

- Example response

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

Status Code

For details, see **Status Codes**.

7.1.13 Querying Listeners by Tag

Function

This API is used to query listeners by tag.

Constraints

None

URI

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

Table 7-51 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the ID of the project where the tag is used.

Request Parameters

Table 7-52 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token

Table 7-53 Parameter description

Parameter	Mandatory	Type	Description
tags	No	Array	A maximum of 20 keys can be queried at a time, and each key can contain a maximum of 20 values. The structure body must be included. The tag key cannot be left blank or be an empty string. Each tag key and each tag value of the same tag key must be unique. For details, see **Table 7-54**.
limit	No	Integer	Sets the page size. This parameter is available when **action** is set to **filter**. Both the default value and maximum value are **1000**, and the minimum value is **1**. The value cannot be a negative integer.
offset	No	Integer	Specifies the index position. The query starts from the next listener indexed by this parameter. This parameter is not required when you query listeners on the first page. The value in the response returned for querying the listeners on the previous page will be included in this parameter for querying the listeners 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 positive integer, and the default value is **0**.
action	Yes	String	Identifies the operation. The value can be **filter** or **count**. • **filter**: indicates pagination query. • **count**: indicates that all listeners meeting the search criteria will be returned.

Parameter	Mandatory	Type	Description
matches	No	Array	Specifies the search criteria. The tag key is the parameter to match, for example, **resource_name**. **value** indicates the value of the match content. The key is a fixed dictionary value. Determine whether fuzzy match is required based on different parameters. For example, if the **key** is **resource_name**, fuzzy search is used by default. If **value** is an empty string, exact match is used. If the key is **resource_id**, exact match is used. For details, see **Table 7-55**.

Table 7-54 tags parameter description

Parameter	Mandatory	Type	Description
key	Yes	String	Specifies the tag key. It contains a maximum of 128 Unicode characters and cannot be left blank. (This parameter is not verified in the search process.)
values	Yes	Array	Lists the tag values. Each tag value can contain a maximum of 255 Unicode characters. The values are in the OR relationship.

Table 7-55 matches parameter description

Parameter	Mandatory	Type	Description
key	Yes	String	Specifies the tag key. The value can be one of the following: • **resource_name**: indicates the resource name. • **resource_id**: indicates the resource ID.
value	Yes	String	Specifies the tag value. Each tag value can contain a maximum of 255 Unicode characters.

Response Parameters

Table 7-56 Response parameters

Parameter	Type	Description
resources	Array	Lists the listeners. For details, see **Table 7-57**.
total_count	Integer	Specifies the total number of queried records.

Table 7-57 resource parameter description

Parameter	Type	Description
resource_id	String	Specifies the resource ID.
resource_detail	String	Specifies the resource details. The value is a resource object, used for extension. The value is left blank by default.
tags	Array	Lists the tags. If there is no tag, an empty array is used by default. For details, see **Table 7-58**.
resource_name	String	Specifies the resource name. This parameter is an empty string by default if there is no resource name.
super_resource_id	String	Specifies the parent resource ID.

Table 7-58 tags parameter description

Parameter	Type	Description
key	String	Specifies the tag key. It contains a maximum of 128 Unicode characters and cannot be left blank. (This parameter is not verified in the search process.)
value	String	Specifies the tag value. Each tag value can contain a maximum of 255 Unicode characters.

Example Request

- Example request 1 (when **action** is set to **filter**)
  POST https://{Endpoint}/v2.0/6a0de1c3-7d74-4f4a-b75e-e57135bd2b97/listeners/resource_instances/action


```
{
   "offset": "100",
   "limit": "100",
   "action": "filter",
   "matches": [
      {
         "key": "resource_name",
         "value": "resource1"
      }
   ],
   "tags": [
      {
         "key": "key1",
         "values": [
            "value1",
            "value2"
         ]
      }
   ]
}
```

- Example request 2 (when **action** is set to **count**)

```
POST https://{Endpoint}/v2.0/6a0de1c3-7d74-4f4a-b75e-e57135bd2b97/listeners/resource_instances/action

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

Example Response

- Example response 1

```
{
   "resources": [
      {
         "resource_detail":"",
         "resource_id": "154d135b-3a89-4e89-8023-06efb9acdc05",
         "resource_name": "resouece1",
         "tags": [
            {
               "key": "key1",
               "value": "value1"
            },
            {
               "key": "key2",
               "value": "value1"
```



```
            }
          ]
        }
    ],
    "total_count": 1000
}
```

- Example response 2

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

Status Code

For details, see **Status Codes**.

7.1.14 Deleting a Tag from a Listener

Function

This API is used to delete a tag with a specific key from a listener.

Constraints

None

URI

DELETE /v2.0/{project_id}/listeners/{listener_id}/tags/{key}

Table 7-59 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the ID of the project where the tag is used.
listener_id	Yes	String	Specifies the ID of the listener from which a tag is to be deleted.

Request Parameters

Table 7-60 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token

Response Parameters

None

Example Request

- Example request
  DELETE https://{Endpoint}/v2.0/6a0de1c3-7d74-4f4a-b75e-e57135bd2b97/listeners/7add33ad-11dc-4ab9-a50f-419703f13163/tags/key1

Example Response

- Example response
  None

Status Code

For details, see **Status Codes**.

7.1.15 Status Codes

Table 7-61 Normal codes

Status Code	Message	Description
200	OK	Specifies the normal response code for the GET operation. This code is returned when a response body is returned for the POST operation.
204	No Content	Specifies the normal response code for the DELETE operation. This code is returned when no response body is returned for the POST operation.

Table 7-62 Error codes

Status Code	Error Code	Description	Error Message	Measure
400	VPC.1801	The ID is incorrect.	resource id is invalid/ Getting id is invalid.	Use a correct resource ID.
400	VPC.1801	An action error occurs.	action is invalid.	Ensure that the value of **action** is **create** or **delete**.

Status Code	Error Code	Description	Error Message	Measure
400	VPC.1801	The key length is invalid.	Tag length is invalid. The key length must be in range [1,36] and value in range [0,43]	Input a valid key.
400	VPC.0007	The project ID is incorrect.	urlTenantId is not equal token TenantId.	Check the project ID.
401	VPC.0008	The token in the request is invalid or the request does not contain the token.	Invalid token in the header./ Authorization information is wrong.	Check whether the token is valid.
400	VPC.1801	The value length is invalid.	Tag length is invalid. The key length must be in range [1,36] and value in range [0,43]	Input a valid value.
400	VPC.1801	The key or value contains invalid characters.	InvalidInput/Tag value xxx is invalid.	Check the validity of the key or value.
400	VPC.1801	The key or value is left blank.	Tag xxx can not be null.	Check whether the key or value is left blank.
400	VPC.1801	The tag is null.	Tag can not be null.	Check whether the tag is null.
400	VPC.1801	A resource type error occurs.	Resource xxx is invalid.	Ensure that the value of **resource_type** is **loadbalancers** or **listeners**.

Status Code	Error Code	Description	Error Message	Measure
400	VPC.1801	The total number of tags added at a time exceeds 10.	number of tags exceeds max unm of 10.	Reduce the number of tags.
400	VPC.1814	The total number of existing tags and newly added tags exceeds 10.	Invalid input for operation: resource_id: XXXX, number of tags exceed max num of 10.	Reduce the number of tags.
400	VPC.1814	The key values of newly added tags are duplicate.	Invalid input for operation: tags key is duplicated.	Change the tag values.
400	VPC.1814	The resource ID does not exist.	Resource XXX XXX could not be found.	Check whether the resource is available.
400	VPC.1814	The specified key to be deleted does not exist, or the key is an empty string.	The resource could not be found.	Enter a correct key and send the request again.
400	VPC.1814	More than 10 tags are added to a specified resource.	Invalid input for operation:resource_id:xxx, number of tags exceeds max num of 10.	Each resource supports up to 10 tags.
400	VPC.1801	Tags are duplicate.	Tag key is repeated.	Delete duplicate tags and resend the request.
500	-	The request format is incorrect.	Internal Server Error.	Use the correct request body format.

8 Examples

8.1 Creating a Dedicated Load Balancer and Binding a New EIP to It

Scenarios

Call APIs to create a dedicated load balancer and bind a new EIP to it.

Prerequisites

You have created a VPC and a subnet.

Procedure

1. Query the subnet you have created.
   a. Send **GET https://*{vpc_endpoint}*/v1/*{project_id}*/subnets**. *project_id* indicates the project ID.
   b. Add **X-Auth-Token** to the request header.
   c. Check the response.
      - The request is successful if the following response is displayed:

```
{
   "subnets": [
   {
         "id": "0535759e-8104-49d9-902c-a05185a94bdf", // Subnet ID
         "name": "subnet-001", // Subnet name
         "description": "",
         "cidr": "172.16.66.0/24", //IPv4 address range
         "dnsList": [
            "100.125.4.6"
         ],
         "status": "ACTIVE",
         "vpc_id": "44789a9f-3e80-451a-ac03-0818f99b6cdd", // VPC ID
         "ipv6_enable": true,
         "gateway_ip_v6": "2001:db8:a583:37c::1",
         "cidr_v6": "2001:db8:a583:37c::/64",
         "gateway_ip": "172.16.66.1",
         "dhcp_enable": true,
         "primary_dns": "100.125.4.6",
         "availability_zone": "eu-de-01", //AZ of the subnet
```



```
        "neutron_network_id": "0535759e-8104-49d9-902c-a05185a94bdf", // Network ID
        "neutron_subnet_id": "1492f0ba-cfce-4e2c-86f7-561d757dfeee", // IPv4 subnet ID
        "neutron_subnet_id_v6": "3c052475-b50b-49b9-abb1-558bad45e592",
        "extra_dhcp_opts": [
          {
            "opt_value": "8760h",
            "opt_name": "addresstime"
          }
        ]
      }
    ]
}
```

- If the request is abnormal, locate the fault by referring to **Error Codes**.

2. Create a dedicated load balancer and bind a new EIP to it.
   a. Send **POST https://*{elb_endpoint}*/v3/*{project_id}*/elb/loadbalancers**. *project_id* indicates the project ID.
   b. Add **X-Auth-Token** to the request header.
   c. Ensure that the following parameters, including **publicip**, are passed in the request body:

```
{
  "loadbalancer": {
        "vpc_id": "e5a892ff-3c33-44ef-ada5-b713eb1f7a8b",
        "availability_zone_list": [
          "br-iaas-odin1a"
        ],
        "admin_state_up": true,
        "vip_subnet_cidr_id": "1800b6b8-a69f-4719-813d-24d62aaf32bd",
        "name": "elb-ipv4",
        "publicip": {
          "network_type": "5_bgp",
          "bandwidth": {
            "size": 2,
            "share_type": "PER",
            "charge_mode": "bandwidth",
            "name": "elb_eip_bandwidth"
          }
       }
  }
}
```

   d. Check the response.
      - The request is successful if the following response is displayed:

```
{
  "request_id": "21177eb184c52c5a4540c78dc7fdaee4",
  "loadbalancer": {
    "id": "a2556f92-3310-4173-a6d1-0b2d0bb68478",
    "project_id": "060576782980d5762f9ec014dd2f1148",
    "name": "elb-ipv4",
    "description": "",
    "vip_port_id": "fff961a9-4514-4469-84d4-a2bc4fbdfbeb",
    "vip_address": "192.168.0.162",
    "admin_state_up": true,
    "provisioning_status": "ACTIVE",
    "operating_status": "ONLINE",
    "listeners": [],
    "pools": [],
    "tags": [],
    "provider": "vlb",
    "created_at": "2021-02-23T08:50:19Z",
    "updated_at": "2021-02-23T08:50:19Z",
    "vpc_id": "e5a892ff-3c33-44ef-ada5-b713eb1f7a8b",
    "enterprise_project_id": "0",
    "availability_zone_list": [
```



```
            "br-iaas-odin1a"
        ],
        "ipv6_vip_address": null,
        "ipv6_vip_virsubnet_id": null,
        "ipv6_vip_port_id": null,
        "ipv6_bandwidth": null,
        "publicips": [
            {
                "publicip_id": "12cba100-764e-476c-bf3f-8aba98782cf5",
                "publicip_address": "10.246.173.188",
                "ip_version": 4
            }
        ],
        "elb_virsubnet_ids": [
            "4df3e391-5ebf-4300-b614-cf5a4e793666"
        ],
        "elb_virsubnet_type": "dualstack",
        "ip_target_enable": false,
        "frozen_scene": null,
        "eips": [
            {
                "eip_id": "12cba100-764e-476c-bf3f-8aba98782cf5",
                "eip_address": "10.246.173.188",
                "ip_version": 4
            }
        ],
        "guaranteed": true,
        "billing_info": null,
        "l4_flavor_id": null,
        "l4_scale_flavor_id": null,
        "l7_flavor_id": null,
        "l7_scale_flavor_id": null,
        "vip_subnet_cidr_id": "1800b6b8-a69f-4719-813d-24d62aaf32bd"
    }
}
```


- If the request is abnormal, locate the fault by referring to **Error Codes**.

8.2 Adding a Listener to a Dedicated Load Balancer

Scenarios

Call the API to add a listener to a dedicated load balancer.

Prerequisites

- You have created a dedicated load balancer.
- You have obtained the ID of the dedicated load balancer.

Procedure

1. Add a listener.
   a. Send **POST https://*{elb_endpoint}*/v3/*{project_id}*/elb/listeners**. *project_id* indicates the project ID.
   b. Add **X-Auth-Token** to the request header.
   c. Ensure that the following parameters are passed in the request body:

```
{
    "listener": {
        "protocol_port": 80, // Frontend port. The listener will use this port to receive requests.
```

```
    "protocol": "HTTP", // Frontend protocol. The listener will use this protocol to receive requests.
    "loadbalancer_id": "f77281cb-9f58-4347-8f82-2180d8bea789", // Load balancer that the listener is added to
    "name": "my_listener" // Listener name
  }
}
```

d. Check the response.

- The request is successful if the following response is displayed:

```
{
  "listener": {
    "id": "90ad2705-4ffd-43d3-8f75-af8086bde841",
    "name": "my_listener",
    "protocol_port": 80,
    "protocol": "HTTP",
    "description": "",
    "default_tls_container_ref": null,
    "admin_state_up": true,
    "loadbalancers": [
      {
        "id": "f77281cb-9f58-4347-8f82-2180d8bea789"
      }
    ],
    "client_ca_tls_container_ref": null,
    "project_id": "057ef081eb00d2732fd1c01a9be75e6f",
    "sni_container_refs": [],
    "connection_limit": -1,
    "default_pool_id": null,
    "tls_ciphers_policy": null,
    "tags": [],
    "created_at": "2020-11-21T03:09:13Z",
    "updated_at": "2020-11-21T03:09:13Z",
    "http2_enable": false,
    "insert_headers": {
      "X-Forwarded-ELB-IP": false,
      "X-Forwarded-Host": true,
      "X-Forwarded-For-Port": false,
      "X-Forwarded-Port": false
    },
    "member_timeout": 60,
    "client_timeout": 60,
    "keepalive_timeout": 60,
    "ipgroup": null,
    "enable_member_retry": true,
    "transparent_client_ip_enable": true
  },
  "request_id": "fcd61ee6a6a6c673c65fa0df0577fed9"
}
```

- If the request is abnormal, locate the fault by referring to **Error Codes**.

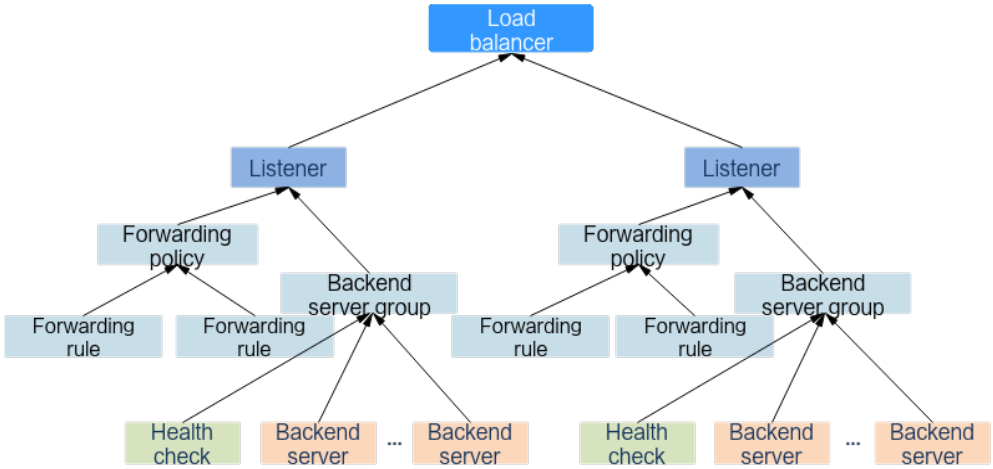
8.3 Deleting a Dedicated Load Balancer

Scenarios

Call APIs to delete a dedicated load balancer.

Before you delete a dedicated load balancer, delete all resources associated with it. **Figure 8-1** shows the associated resources.

Figure 8-1 Resources associated with a dedicated load balancer



Procedure

Perform the following steps to delete the associated resources and the load balancer. Skip the corresponding step if the associated resources do not exist. For example, you can skip **1** if no health check is configured.

1. Delete the health check configured for each associated backend server group.
   a. Send **DELETE https://*{elb_endpoint}*/v3/*{project_id}*/elb/healthmonitors/*{healthmonitor_id}***. *project_id* indicates the project ID, and *healthmonitor_id* indicates the health check ID.
   b. Add **X-Auth-Token** to the request header.
   c. Check the response.
      - If the request is successful, 204 is returned, and the response body is empty.
      - If the request is abnormal, locate the fault by referring to **Error Codes**.
2. Remove backend servers from each associated backend server group.
   a. Send **DELETE https://*{elb_endpoint}*/v3/*{project_id}*/elb/pools/*{pool_id}*/members/*{member_id}***. *project_id* indicates the project ID, *pool_id* indicates the backend server group ID, and **member_id** indicates the backend server ID.
   b. Add **X-Auth-Token** to the request header.
   c. Check the response.
      - If the request is successful, 204 is returned, and the response body is empty.
      - If the request is abnormal, locate the fault by referring to **Error Codes**.
3. Delete each associated backend server group.
   a. Send **DELETE https://*{elb_endpoint}*/v3/{project_id}/elb/pools/*{pool_id}***. *project_id* indicates the project ID, and *pool_id* indicates the backend server group ID.

b. Add **X-Auth-Token** to the request header.

c. Check the response.

- If the request is successful, 204 is returned, and the response body is empty.
- If the request is abnormal, locate the fault by referring to **Error Codes**.

4. Delete the forwarding rules added to each listener.

a. Send **DELETE https://***{elb_endpoint}***/v3/***{project_id}***/elb/l7policies/***{policy_id}***/rules/***{rule_id}*. *project_id* indicates the project ID, *policy_id* indicates the forwarding policy ID, and *rule_id* indicates the forwarding rule ID.

b. Add **X-Auth-Token** to the request header.

c. Check the response.

- If the request is successful, 204 is returned, and the response body is empty.
- If the request is abnormal, locate the fault by referring to **Error Codes**.

5. Delete the forwarding policies added to each listener.

a. Send **DELETE https://***{elb_endpoint}***/v3/***{project_id}***/elb/l7policies/***{policy_id}*. *project_id* indicates the project ID, and *policy_id* indicates the forwarding policy ID.

b. Add **X-Auth-Token** to the request header.

c. Check the response.

- If the request is successful, 204 is returned, and the response body is empty.
- If the request is abnormal, locate the fault by referring to **Error Codes**.

6. Delete each listener added to the load balancer.

a. Send **DELETE https://***{elb_endpoint}***/v3/***{project_id}***/elb/listeners/***{listener_id}*. *project_id* indicates the project ID, and *listener_id* indicates the listener ID.

b. Add **X-Auth-Token** to the request header.

c. Check the response.

- If the request is successful, 204 is returned, and the response body is empty.
- If the request is abnormal, locate the fault by referring to **Error Codes**.

7. Delete the load balancer.

a. Send **DELETE https://***{elb_endpoint}***/v3/***{project_id}***/elbloadbalancers/***{loadbalancer_id}*. *project_id* indicates the project ID, and *loadbalancer_id* indicates the load balancer ID.

b. Add **X-Auth-Token** to the request header.

c. Check the response.

- If the request is successful, 204 is returned, and the response body is empty.
- If the request is abnormal, locate the fault by referring to **Error Codes**.

8.4 Creating a Public Network (Shared) Load Balancer

Scenarios

Call APIs to create a load balancer and bind a new EIP to it.

Prerequisites

You have created a VPC and a subnet.

Procedure

Bind an EIP to the port that has been bound to the private IP address of the load balancer based on **Example request 1: Creating a private network load balancer**. For details about the parameters, see **Table 8-1**.

Table 8-1 Request parameters

Parameter	Mandatory	Type	Description
publicip	Yes	Object	Specifies the EIP. For details, see **Table 8-2**.
bandwidth	Yes	Object	Specifies the bandwidth. For details, see **Table 8-3**.
enterprise_project_id	No	String	• Specifies the enterprise project ID. The value is **0** or a UUID that can contain a maximum of 36 characters, including hyphens (-). • When assigning an EIP, you need to bind an enterprise project ID to the EIP. • If this parameter is not specified, the default value is **0**. **NOTE** For more information about enterprise projects and how to obtain enterprise project IDs, see **Enterprise Management User Guide**.

Table 8-2 publicip parameter description

Parameter	Mandatory	Type	Description
type	Yes	String	• Specifies the EIP type. • The value can be **5_telcom**, **5_union**, **5_bgp**, or **5_sbgp**. – CN South-Guangzhou: **5_bgp** and **5_sbgp** – CN East-Shanghai2: **5_bgp** and **5_sbgp** – CN North-Beijing1: **5_bgp** and **5_sbgp** – CN-Hong Kong: **5_bgp** – CN Southwest-Guiyang1: **5_bgp** and **5_sbgp** – CN North-Beijing4: **5_bgp** and **5_sbgp** • Note: – The configured value must be supported by the system. – **publicip_id** is an IPv4 port. If **publicip_type** is not specified, the default value is **5_bgp**.
ip_version	No	Integer	• Specifies the EIP version. • The value can be **4** and **6**. **4** indicates an IPv4 address, and **6** indicates an IPv6 address. • Note: – The configured value must be supported by the system. – If this parameter is left blank or is an empty string, an IPv4 address is assigned by default.

Parameter	Mandatory	Type	Description
ip_address	No	String	• Specifies the EIP to be assigned. The system automatically assigns an EIP if you do not specify it. • The value must be a valid IPv4 address in the available IP address range.

Table 8-3 bandwidth parameter description

Parameter	Mandatory	Type	Description
name	No	String	• Specifies the bandwidth name. • The value can contain 1 to 64 characters that can contain letters, digits, underscores (_), hyphens (-), and periods (.). • This parameter is mandatory when **share_type** is set to **PER**. This parameter will be ignored when **share_type** is set to **WHOLE** with an ID specified.

Parameter	Mandatory	Type	Description
size	No	Integer	• Specifies the bandwidth (Mbit/s). • The value ranges from **1** to **300** by default (The specific range may vary depending on the configuration in each region. You can see the bandwidth range of each region on the management console.) • This parameter is mandatory when **share_type** is set to **PER**. This parameter will be ignored when **share_type** is set to **WHOLE** with an ID specified. • The minimum unit for bandwidth adjustment varies depending on the bandwidth range. The details are as follows: – The minimum increment is 1 Mbit/s if the allowed bandwidth ranges from 0 to 300 Mbit/s. – The minimum increment is 50 Mbit/s if the allowed bandwidth ranges from 301 Mbit/s to 1000 Mbit/s. – The minimum increment is 500 Mbit/s if the allowed bandwidth is greater than 1,000 Mbit/s.
id	No	String	• Specifies the bandwidth ID. You can specify an existing shared bandwidth when assigning an EIP. • The value can be the ID of the shared bandwidth whose type is set to **WHOLE**.

Parameter	Mandatory	Type	Description
share_type	Yes	String	• Specifies the bandwidth type. • The value can be one of the following: – **PER**: indicates dedicated bandwidth. – **WHOLE**: indicated shared bandwidth.
charge_mode	No	String	• The default value is **traffic**. Currently, only billing by traffic is supported.

- Step 1: Apply for an EIP.

```
POST https://{VPCEndpoint}/v1/8b7e35ad379141fc9df3e178bd64f55c/publicips

{
   "publicip": {
      "type": "5_bgp",
      "ip_version": 4
   },
   "bandwidth": {
      "name": "bandwidth123",
      "size": 10,
      "share_type": "PER"
   }
}
```

- Example response

```
{
   "publicip": {
      "id": "f588ccfa-8750-4d7c-bf5d-2ede24414706",
      "status": "PENDING_CREATE",
      "type": "5_bgp",
      "public_ip_address": "139.9.204.183",
      "tenant_id": "8b7e35ad379141fc9df3e178bd64f55c",
      "ip_version": 4,
      "create_time": "2019-06-29 06:45:32",
      "bandwidth_size": 1

   }
}
```

- Step 2: Bind the EIP. (The value of **public_id** is the same as that in the ▪ **Example response**, and the value of **port_id** is the same as that of **vip_port_id** in **Example response 1**.)

```
PUT /v1/8b7e35ad379141fc9df3e178bd64f55c/publicips/f588ccfa-8750-4d7c-bf5d-2ede24414706

{
   "publicip": {
      "port_id": "a7ecbdb5-5a63-41dd-a830-e16c0a7e04a7"
   }
}
```

- Example response

```
{
  "publicip": {
    "id": "f588ccfa-8750-4d7c-bf5d-2ede24414706",
    "status": "ACTIVE",
    "type": "5_bgp",
    "port_id": "a7ecbdb5-5a63-41dd-a830-e16c0a7e04a7",
```



```
  "public_ip_address": "139.9.204.183",
  "private_ip_address": "192.168.1.131",
  "tenant_id": "8b7e35ad379141fc9df3e178bd64f55c",
  "create_time": "2019-06-29 07:33:18",
  "bandwidth_size": 1,
  "ip_version": 4
 }
}
```

- After the preceding steps are complete, the load balancer has the capability of accessing the public network. You can access the load balancer using 139.9.204.183, the value of parameter **public_ip_address**.

8.5 Querying the ID of an ECS Used as a Backend Server

Scenarios

Call APIs to obtain the ID of an ECS used as a backend server of a load balancer.

Prerequisites

You have created a load balancer, a backend server group, and a backend server.

Procedure

Send **GET /v3/*{project_id}*/elb/members**. *project_id* indicates the project ID. You can add other criteria as you needed. For details, see the API document. Add **X-Auth-Token** to the request header.

View the response result and obtain the ECS ID from **instance_id**.

- The request is successful if the following response is displayed:

```
{
   "request_id": "0df89f0ad2ecf0e0a5688978d28e9a6d",
   "members": [
      {
         "weight": 1,
         "admin_state_up": true,
         "project_id": "04dd36f9c0000fe22f9fc00b409f1sq1",
         "address": "192.168.2.96",
         "protocol_port": 80,
         "id": "0b7c1e58-5940-41c1-a7c5-dbe4b3f23e4w",
         "operating_status": ONLINE,
         "status": [
            {
               "listener_id": "73bea9d6-fb7f-47cc-b949-c3382abb1f46",
               "operating_status": "ONLINE"
            }
         ],
         "instance_id": "6985a0dc-5884-40f2-9426-15fb4bab8f1d", // ECS ID
         "device_id": "6985a0dc-5884-40f2-9426-15fb4bab8f1d",
         "device_owner": "compute:az1",
         "member_type": "instance",
         "created_at": "2023-05-15T07:15:43Z",
         "updated_at": "2023-05-15T07:15:53Z",
         "loadbalancer_id": "955af176-4275-49ac-b47e-05912x9dj33c",
         "loadbalancers": [
            {
               "id": "955af176-4275-49ac-b47e-05912x9dj33c"
            }
         ],
```



```
            "pool_id": "b6e6fdcf-4f4d-4d21-95ca-925143af6de8",
            "ip_version": "v4",
            "subnet_cidr_id": "b765590e-905e-4e13-9d34-0e0ea9de2k9d"
        }
    ],
    "page_info": {
        "previous_marker": "0b7c1e58-5940-41c1-a7c5-dbe4b3f83506",
        "current_count": 1
    }
}
```


- If the request is abnormal, locate the fault by referring to **Error Codes**.

9 Permissions and Supported Actions

9.1 Introduction

This section describes fine-grained permissions management for ELB. If your Huawei Cloud account does not need individual IAM users, then you may skip this chapter.

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from the groups to which they are added and can perform specified operations on cloud services based on the permissions.

An account has all of the permissions required to call all APIs, but IAM users must have the required permissions specifically assigned. The permissions required for calling an API are determined by the actions supported by the API. Only users who have been granted permissions allowing the actions can call the API successfully. For example, if an IAM user queries backend servers using an API, the user must have been granted permissions that allow the elb:servers:list action.

Supported Actions

ELB provides system-defined policies that can be directly used in IAM. You can also create custom policies and use them to supplement system-defined policies, implementing more refined access control. Operations supported by policies are specific to APIs. The following are common concepts related to policies:

- Permissions: Defined by actions in a custom policy.
- APIs: REST APIs that can be called in a custom policy.
- Actions: Added to a custom policy to control permissions for specific operations.
- Dependencies: actions which a specific action depends on. When allowing an action for a user, you also need to allow any existing action dependencies for that user.
- IAM projects or enterprise projects: Type of projects in which policies can be used to grant permissions. A policy can be applied to IAM projects, 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 Project. For details about the differences between IAM and enterprise projects, see **Differences Between IAM Projects and Enterprise Projects**

Supported Actions (V3) describes the custom policy authorization items supported by ELB.

- **Load balancer actions**, including actions supported by all load balancer APIs, such as the APIs for creating a load balancer, querying a load balancer, querying the load balancer status tree, querying the load balancer list, updating a load balancer, and deleting a load balancer.

  NOTE

  The check mark (√) indicates that an action takes effect. The cross mark (x) indicates that an action does not take effect.

9.2 Supported Actions (V2)

9.2.1 Load Balancer

Permission	API	Action	IAM Project	Enterprise Project
Creates a load balancer	POST /v2/{project_id}/elb/loadbalancers	elb:loadbalancers:create	√	√
Queries a load balancer	GET /v2/{project_id}/elb/loadbalancers/{loadbalancer_id}	elb:loadbalancers:get	√	√
Queries the status tree of a load balancer	GET /v2/{project_id}/elb/loadbalancers/{loadbalancer_id}/statuses	elb:loadbalancers:get	√	√

Permission	API	Action	IAM Project	Enterprise Project
Queries load balancers	GET /v2/{project_id}/elb/loadbalancers	elb:loadbalancers:list	√	√
Updates a load balancer	PUT /v2/{project_id}/elb/loadbalancers/{loadbalancer_id}	elb:loadbalancers:put	√	√
Deletes a load balancer	DELETE /v2/{project_id}/elb/loadbalancers/{loadbalancer_id}	elb:loadbalancers:delete	√	√

9.2.2 Listener

Permission	API	Action	IAM Project	Enterprise Project
Adds a listener	POST /v2/{project_id}/elb/listeners	elb:listeners:create	√	√
Queries a listener	GET /v2/{project_id}/elb/listeners/{listener_id}	elb:listeners:get	√	√
Queries listeners	GET /v2/{project_id}/elb/listeners	elb:listeners:list	√	√
Modifies a listener	PUT /v2/{project_id}/elb/listeners/{listener_id}	elb:listeners:put	√	√
Deletes a listener	DELETE /v2/{project_id}/elb/listeners/{listener_id}	elb:listeners:delete	√	√

9.2.3 Backend Server Group

Permission	API	Action	IAM Project	Enterprise Project
Adds a backend server group	POST /v2/{project_id}/elb/pools	elb:pools:create	√	√
Queries a backend server group	GET /v2/{project_id}/elb/pools/{pool_id}	elb:pools:get	√	√
Queries backend server groups	GET /v2/{project_id}/elb/pools	elb:pools:list	√	√
Modifies a backend server group	PUT /v2/{project_id}/elb/pools/{pool_id}	elb:pools:put	√	√
Deletes a backend server group	DELETE /v2/{project_id}/elb/pools/{pool_id}	elb:pools:delete	√	√

9.2.4 Backend Server

Permission	API	Action	IAM Project	Enterprise Project
Adds a backend server	POST /v2/{project_id}/elb/pools/{pool_id}/members	elb:members:create	√	√

Permission	API	Action	IAM Project	Enterprise Project
Queries a backend server	GET /v2/{project_id}/elb/pools/{pool_id}/members/{member_id}	elb:members:get	√	√
Queries backend servers	GET /v2/{project_id}/elb/pools/{pool_id}/members	elb:members:list	√	√
Modifies a backend server	PUT /v2/{project_id}/elb/pools/{pool_id}/members/{member_id}	elb:members:put	√	√
Removes a backend server	DELETE /v2/{project_id}/elb/pools/{pool_id}/members/{member_id}	elb:members:delete	√	√

9.2.5 Health Check

Permission	API	Action	IAM Project	Enterprise Project
Configures a health check	POST /v2/{project_id}/elb/healthmonitors	elb:healthmonitors:create	√	√
Queries a health check	GET /v2/{project_id}/elb/healthmonitors/{healthmonitor_id}	elb:healthmonitors:get	√	√
Queries health checks	GET /v2/{project_id}/elb/healthmonitors	elb:healthmonitors:list	√	√
Modifies a health check	PUT /v2/{project_id}/elb/healthmonitors/{healthmonitor_id}	elb:healthmonitors:put	√	√

Permission	API	Action	IAM Project	Enterprise Project
Deletes a health check	DELETE /v2/{project_id}/elb/healthmonitors/{healthmonitor_id}	elb:healthmonitors:delete	√	√

9.2.6 Forwarding Policy

Permission	API	Action	IAM Project	Enterprise Project
Adds a forwarding policy	POST /v2/{project_id}/elb/l7policies	elb:l7policies:create	√	√
Queries a forwarding policy	GET /v2/{project_id}/elb/l7policies/{l7policy_id}	elb:l7policies:get	√	√
Queries forwarding policies	GET /v2/{project_id}/elb/l7policies	elb:l7policies:list	√	√
Updates a forwarding policy	PUT /v2/{project_id}/elb/l7policies/{l7policy_id}	elb:l7policies:put	√	√
Deletes a forwarding policy	DELETE /v2/{project_id}/elb/l7policies/{l7policy_id}	elb:l7policies:delete	√	√

9.2.7 Forwarding Rule

Permission	API	Action	IAM Project	Enterprise Project
Creates a forwarding rule	POST /v2/{project_id}/elb/l7policies/{l7policy_id}/rules	elb:l7rules:create	√	√
Queries a forwarding rule	GET /v2/{project_id}/elb/l7policies/{l7policy_id}/rules/{l7rule_id}	elb:l7rules:get	√	√
Queries forwarding rules	GET /v2/{project_id}/elb/l7policies/{l7policy_id}/rules	elb:l7rules:list	√	√
Updates a forwarding rule	PUT /v2/{project_id}/elb/l7policies/{l7policy_id}/rules/{l7rule_id}	elb:l7rules:put	√	√
Deletes a forwarding rule	DELETE /v2/{project_id}/elb/l7policies/{l7policy_id}/rules/{l7rule_id}	elb:l7rules:delete	√	√

9.2.8 Whitelist

Permission	API	Action	IAM Project	Enterprise Project
Adds a whitelist	POST /v2/{project_id}/elb/whitelists	elb:whitelists:create	√	√
Queries a whitelist	GET /v2/{project_id}/elb/whitelists/{whitelist_id}	elb:whitelists:get	√	√

Permission	API	Action	IAM Project	Enterprise Project
Queries whitelists	GET /v2/{project_id}/elb/whitelists	elb:whitelists:list	√	√
Modifies a whitelist	PUT /v2/{project_id}/elb/whitelists/{whitelist_id}	elb:whitelists:put	√	√
Deletes a whitelist	DELETE /v2/{project_id}/elb/whitelists/{whitelist_id}	elb:whitelists:delete	√	√

9.2.9 SSL Certificate

Permission	API	Action	IAM Project	Enterprise Project
Creates a certificate	POST /v2/{project_id}/elb/certificates	elb:certificates:create	√	√
Queries a certificate	GET /v2/{project_id}/elb/certificates/{certificate_id}	elb:certificates:get	√	√
Queries certificates	GET /v2/{project_id}/elb/certificates	elb:certificates:list	√	√
Modifies a certificate	PUT /v2/{project_id}/elb/certificates/{certificate_id}	elb:certificates:put	√	√
Deletes a certificate	DELETE /v2/{project_id}/elb/certificates/{certificate_id}	elb:certificates:delete	√	√

9.2.10 Quota

Permission	API	Action	IAM Project	Enterprise Project
Queries default resource quotas	GET /v2/{project_id}/elb/quotas/defaults	elb:quotas:list	√	x
Queries current resource quotas	GET /v2/{project_id}/elb/quotas	elb:quotas:list	√	x

9.2.11 Tag

Permission	API	Action	IAM Project	Enterprise Project
Queries all tags of a load balancer.	GET /v2.0/{project_id}/loadbalancers/{loadbalancer_id}/tags	elb:loadbalancerTags:get	√	x
Adds or deletes load balancer tags in batches.	POST /v2.0/{project_id}/loadbalancers/{loadbalancer_id}/tags/action	elb:loadbalancerTags:create	√	x
Queries tags of all load balancers in a specific project.	GET /v2.0/{project_id}/loadbalancers/tags	elb:loadbalancerTags:get	√	x

Permission	API	Action	IAM Project	Enterprise Project
Queries load balancers by tag.	POST /v2.0/{project_id}/loadbalancers/resource_instances/action	elb:loadbalancerTags:get	√	x
Adds a tag to a specific load balancer.	POST /v2.0/{project_id}/loadbalancers/{loadbalancer_id}/tags	elb:loadbalancerTags:create	√	x
Deletes a tag with a specific key from a load balancer.	DELETE /v2.0/{project_id}/loadbalancers/{loadbalancer_id}/tags/{key}	elb:loadbalancerTags:delete	√	x
Queries all tags of a listener.	GET /v2.0/{project_id}/listeners/{listener_id}/tags	elb:listenerTags:get	√	x
Adds or deletes listener tags in batches.	POST /v2.0/{project_id}/listeners/{listener_id}/tags/action	elb:listenerTags:create	√	x
Queries the tags of all listeners.	GET /v2.0/{project_id}/listeners/tags	elb:listenerTags:get	√	x
Queries listeners by tag.	POST /v2.0/{project_id}/listeners/resource_instances/action	elb:listenerTags:get	√	x
Adds a tag to a specific listener.	POST /v2.0/{project_id}/listeners/{listener_id}/tags	elb:listenerTags:create	√	x
Deletes a tag with a specific key from a listener.	DELETE /v2.0/{project_id}/listeners/{listener_id}/tags/{key}	elb:listenerTags:delete	√	x

9.2.12 Precautions for API Permissions

elb:quotas:list controls the fine-grained permission for quota display.

elb:logtanks:create, **elb:logtanks:list**, **elb:logtanks:get**, **elb:logtanks:put**, and **elb:logtanks:delete** control the fine-grained permission for log creation, log list query, log details query, log update, and log deletion.

The logging function relies on LTS, and the **lts:*:get*** and **lts:*:list*** permissions at the project level are required.

The monitoring function relies on Cloud Eye.

9.3 Supported Actions (V3)

9.3.1 Load Balancer

Permission	API	Action	IAM Project	Enterprise Project
Creates a load balancer	POST /v3/{project_id}/elb/loadbalancers	elb:loadbalancers:create	√	√
Queries a load balancer	GET /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}	elb:loadbalancers:get	√	√
Queries the status tree of a load balancer	GET /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}/statuses	elb:loadbalancers:get	√	√
Queries load balancers	GET /v3/{project_id}/elb/loadbalancers	elb:loadbalancers:list	√	√
Updates a load balancer	PUT /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}	elb:loadbalancers:put	√	√

Permission	API	Action	IAM Project	Enterprise Project
Deletes a load balancer	DELETE /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}	elb:loadbalancers:delete	√	√

9.3.2 Listener

Permission	API	Action	IAM Project	Enterprise Project
Adds a listener	POST /v3/{project_id}/elb/listeners	elb:listeners:create	√	√
Queries a listener	GET /v3/{project_id}/elb/listeners/{listener_id}	elb:listeners:get	√	√
Queries listeners	GET /v3/{project_id}/elb/listeners	elb:listeners:list	√	√
Modifies a listener	PUT /v3/{project_id}/elb/listeners/{listener_id}	elb:listeners:put	√	√
Deletes a listener	DELETE /v3/{project_id}/elb/listeners/{listener_id}	elb:listeners:delete	√	√

9.3.3 Backend Server Group

Permission	API	Action	IAM Project	Enterprise Project
Creates a backend server group	POST /v3/{project_id}/elb/pools	elb:pools:create	√	√

Permission	API	Action	IAM Project	Enterprise Project
Queries a backend server group	GET /v3/{project_id}/elb/pools/{pool_id}	elb:pools:get	√	√
Queries backend server groups	GET /v3/{project_id}/elb/pools	elb:pools:list	√	√
Modifies a backend server group	PUT /v3/{project_id}/elb/pools/{pool_id}	elb:pools:put	√	√
Deletes a backend server group	DELETE /v3/{project_id}/elb/pools/{pool_id}	elb:pools:delete	√	√

9.3.4 Backend Server

Permission	API	Action	IAM Project	Enterprise Project
Adds a backend server	POST /v3/{project_id}/elb/pools/{pool_id}/members	elb:members:create	√	√
Queries a backend server	GET /v3/{project_id}/elb/pools/{pool_id}/members/{member_id}	elb:members:get	√	√

Permission	API	Action	IAM Project	Enterprise Project
Queries backend servers	GET /v3/{project_id}/elb/pools/{pool_id}/members	elb:members:list	√	√
Modifies a backend server	PUT /v3/{project_id}/elb/pools/{pool_id}/members/{member_id}	elb:members:put	√	√
Removes a backend server	DELETE /v3/{project_id}/elb/pools/{pool_id}/members/{member_id}	elb:members:delete	√	√

9.3.5 Health Check

Permission	API	Action	IAM Project	Enterprise Project
Configures a health check	POST /v3/{project_id}/elb/healthmonitors	elb:healthmonitors:create	√	√
Queries a health check	GET /v3/{project_id}/elb/healthmonitors/{healthmonitor_id}	elb:healthmonitors:get	√	√
Queries health checks	GET /v3/{project_id}/elb/healthmonitors	elb:healthmonitors:list	√	√
Modifies a health check	PUT /v3/{project_id}/elb/healthmonitors/{healthmonitor_id}	elb:healthmonitors:put	√	√
Deletes a health check	DELETE /v3/{project_id}/elb/healthmonitors/{healthmonitor_id}	elb:healthmonitors:delete	√	√

9.3.6 Forwarding Policy

Permission	API	Action	IAM Project	Enterprise Project
Adds a forwarding policy	POST /v3/{project_id}/elb/l7policies	elb:l7policies:create	√	√
Queries a forwarding policy	GET /v3/{project_id}/elb/l7policies/{l7policy_id}	elb:l7policies:get	√	√
Queries forwarding policies	GET /v3/{project_id}/elb/l7policies	elb:l7policies:list	√	√
Updates a forwarding policy	PUT /v3/{project_id}/elb/l7policies/{l7policy_id}	elb:l7policies:put	√	√
Deletes a forwarding policy	DELETE /v3/{project_id}/elb/l7policies/{l7policy_id}	elb:l7policies:delete	√	√

9.3.7 Forwarding Rule

Permission	API	Action	IAM Project	Enterprise Project
Creates a forwarding rule	POST /v3/{project_id}/elb/l7policies/{l7policy_id}/rules	elb:l7rules:create	√	√
Queries a forwarding rule	GET /v3/{project_id}/elb/l7policies/{l7policy_id}/rules/{l7rule_id}	elb:l7rules:get	√	√

Permission	API	Action	IAM Project	Enterprise Project
Queries forwarding rules	GET /v3/{project_id}/elb/l7policies/{l7policy_id}/rules	elb:l7rules:list	√	√
Updates a forwarding rule	PUT /v3/{project_id}/elb/l7policies/{l7policy_id}/rules/{l7rule_id}	elb:l7rules:put	√	√
Deletes a forwarding rule	DELETE /v3/{project_id}/elb/l7policies/{l7policy_id}/rules/{l7rule_id}	elb:l7rules:delete	√	√

9.3.8 IP Address Group

Permission	API	Action	IAM Project	Enterprise Project
Creates an IP address group	POST /v3/{project_id}/elb/ipgroups	elb:ipgroups:create	√	√
Queries an IP address group	GET /v3/{project_id}/elb/ipgroups/{ipgroup_id}	elb:ipgroups:get	√	√
Queries IP address groups	GET /v3/{project_id}/elb/ipgroups	elb:ipgroups:list	√	√
Updates an IP address group	PUT /v3/{project_id}/elb/ipgroups/{ipgroup_id}	elb:ipgroups:put	√	√

Permission	API	Action	IAM Project	Enterprise Project
Deletes an IP address group	DELETE /v3/{project_id}/elb/ipgroups/{ipgroup_id}	elb:ipgroups:delete	√	√
Updates IP addresses in an IP address group	PUT /v3/{project_id}/elb/ipgroups/{ipgroup_id}/iplist/create-or-update	elb:ipgroups:put	√	√
Deletes IP addresses in an IP address group	DELETE /v3/{project_id}/elb/ipgroups/{ipgroup_id}/iplist/batch-delete	elb:ipgroups:put	√	√

9.3.9 Certificate

Permission	API	Action	IAM Project	Enterprise Project
Creates a certificate	POST /v3/{project_id}/elb/certificates	elb:certificates:create	√	√
Queries a certificate	GET /v3/{project_id}/elb/certificates/{certificate_id}	elb:certificates:get	√	√
Queries certificates	GET /v3/{project_id}/elb/certificates	elb:certificates:list	√	√
Modifies a certificate	PUT /v3/{project_id}/elb/certificates/{certificate_id}	elb:certificates:put	√	√

Permission	API	Action	IAM Project	Enterprise Project
Deletes a certificate	DELETE /v3/{project_id}/elb/certificates/{certificate_id}	elb:certificates:delete	√	√

9.3.10 Security Policy

Permission	API	Action	IAM Project	Enterprise Project
Creates a custom security policy	POST /v3/{project_id}/elb/security-policies	elb:security-policies:create	√	√
Queries a custom security policy	GET /v3/{project_id}/elb/security-policies/{certificate_id}	elb:security-policies:get	√	√
Queries custom security policies	GET /v3/{project_id}/elb/security-policies	elb:security-policies:list	√	√
Updates a custom security policy	PUT /v3/{project_id}/elb/security-policies/{certificate_id}	elb:security-policies:put	√	√

Permission	API	Action	IAM Project	Enterprise Project
Deletes a custom security policy	DELETE /v3/{project_id}/elb/security-policies/{certificate_id}	elb:security-policies:delete	√	√
Queries system security policies	GET /v3/{project_id}/elb/system-security-policies	elb:security-policies:list	√	√

9.3.11 Quota

Permission	API	Action	IAM Project	Enterprise Project
Queries current resource quotas	GET /v3/{project_id}/elb/quotas	elb:quotas:list	√	√
Queries quota usage	GET /v3/{project_id}/elb/quotas/details	elb:quotas:list	√	√

9.3.12 API Version

Permission	API	Action	IAM Project	Enterprise Project
Queries the API version	GET /versions	elb:quotas:list	√	x

9.3.13 Availability Zone

Permission	API	Action	IAM Project	Enterprise Project
Queries AZs	GET /v3/{project_id}/elb/availability-zones	elb:availability-zones:list	√	√

9.3.14 Load Balancer Flavor

Permission	API	Action	IAM Project	Enterprise Project
Queries default resource quotas	GET /v3/{project_id}/elb/flavors	elb:flavors:list	√	x
Queries current resource quotas	GET /v3/{project_id}/elb/flavors/{flavor_id}	elb:flavors:get	√	x

9.3.15 Precautions for API Permissions

elb:quotas:list controls the fine-grained permission for quota display.

elb:logtanks:create, **elb:logtanks:list**, **elb:logtanks:get**, **elb:logtanks:put**, and **elb:logtanks:delete** control the fine-grained permission for log creation, log list query, log details query, log update, and log deletion.

The logging function relies on LTS, and the **lts:*:get*** and **lts:*:list*** permissions at the project level are required.

The monitoring function relies on Cloud Eye.

10 Historical APIs

10.1 Shared Load Balancer APIs (OpenStack) (Discarded)

10.1.1 Load Balancer

10.1.1.1 Creating a Load Balancer

Function

This API is used to create a private network load balancer. After the load balancer is created, its details, such as load balancer ID, IP address, and subnet ID, are returned.

To create a public network load balancer, you also need to call the API for assigning an EIP and associate this IP address to the port bound to the IP address of the private network load balancer.

URI

POST /v2.0/lbaas/loadbalancers

Request

Table 10-1 Parameter description

Parameter	Mandatory	Type	Description
loadbalancer	Yes	Object	Specifies the load balancer. For details, see **Table 10-2**.

Table 10-2 loadbalancer parameter description

Parameter	Mandatory	Type	Description
name	No	String	Specifies the load balancer name. The value contains a maximum of 255 characters.
description	No	String	Provides supplementary information about the load balancer. The value contains a maximum of 255 characters.
tenant_id	No	String	Specifies the ID of the project where the load balancer is used. The value contains a maximum of 255 characters. The value must be the same as the value of **project_id** in the token.
project_id	No	String	Specifies the ID of the project to which the load balancer belongs. This parameter has the same meaning as **tenant_id**. The value must be the same as the value of **project_id** in the token.
vip_subnet_id	Yes	String	Specifies the ID of the IPv4 subnet where the load balancer works. You can obtain the value by calling the API for querying subnets ({VPC endpoint}/v2.0/subnets) using the GET method. The private IP address of the load balancer is in this subnet. Only IPv4 subnets are supported.
provider	No	String	Specifies the provider of the load balancer. The value can only be **vlb**.
vip_address	No	String	Specifies the private IP address of the load balancer. This IP address must be the one in the subnet specified by **vip_subnet_id**. If this parameter is not specified, an IP address is automatically assigned to the load balancer from the subnet specified by **vip_subnet_id**. The value contains a maximum of 64 characters.

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Specifies the administrative status of the load balancer. This parameter is reserved, and the default value is **true**.

Response

Table 10-3 Response parameters

Parameter	Type	Description
loadbalancer	Object	Specifies the load balancer. For details, see **Table 10-4**.

Table 10-4 loadbalancer parameter description

Parameter	Type	Description
id	String	Specifies the load balancer ID.
project_id	String	Specifies the ID of the project to which the load balancer belongs. This parameter has the same meaning as **tenant_id**.
tenant_id	String	Specifies the ID of the project where the load balancer is used. The value contains a maximum of 255 characters.
name	String	Specifies the load balancer name. The value contains a maximum of 255 characters.
description	String	Provides supplementary information about the load balancer. The value contains a maximum of 255 characters.
vip_subnet_id	String	Specifies the ID of the IPv4 subnet where the load balancer works.

Parameter	Type	Description
vip_port_id	String	Specifies the ID of the port bound to the private IP address of the load balancer. When you create a load balancer, the system automatically creates a port and associates it with a security group. However, the security group will not take effect.
provider	String	Specifies the provider of the load balancer.
vip_address	String	Specifies the private IP address of the load balancer. The value contains a maximum of 64 characters.
listeners	Array	Lists the IDs of listeners added to the load balancer. For details, see **Table 10-5**.
pools	Array	Lists the IDs of backend server groups associated with the load balancer. For details, see **Table 10-6**.
operating_status	String	Specifies the operating status of the load balancer. This parameter is reserved, and its value can be **ONLINE** or **FROZEN**.
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the load balancer.
admin_state_up	Boolean	Specifies the administrative status of the load balancer. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
tags	Array	Lists load balancer tags.

Parameter	Type	Description
created_at	String	Specifies the time when the load balancer was created. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format. The value contains a maximum of 19 characters.
updated_at	String	Specifies the time when the load balancer was updated. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format. The value contains a maximum of 19 characters.

Table 10-5 listeners parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated listener.

Table 10-6 pools parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated backend server group.

Example Request

- Example request 1: Creating a private network load balancer

```
POST https://{Endpoint}/v2.0/lbaas/loadbalancers

{
   "loadbalancer": {
      "name": "loadbalancer1",
      "description": "simple lb",
      "tenant_id": "1867112d054b427e808cc6096d8193a1",
      "vip_subnet_id": "58077bdb-d470-424b-8c45-2e3c65060a5b",
      "vip_address": "192.168.0.100",
      "admin_state_up": true
   }
}
```

- Example request 2

  Bind an EIP to the port that has been bound to the load balancer's private IP address based on **Example request 1: Creating a private network load balancer**. For details about the parameters, see **Table 10-7**.

Table 10-7 Request parameters

Parameter	Mandatory	Type	Description
publicip	Yes	Object	Specifies the EIP. For details, see **Table 10-8**.
bandwidth	Yes	Object	Specifies the bandwidth. For details, see **Table 10-9**.
enterprise_project_id	No	String	• Specifies the enterprise project ID. The value is **0** or a UUID that can contain a maximum of 36 characters, including hyphens (-). • When assigning an EIP, you need to bind an enterprise project ID to the EIP. • If this parameter is not specified, the default value is **0**. **NOTE** For more information about enterprise projects and how to obtain enterprise project IDs, see **Enterprise Management User Guide**.

Table 10-8 publicip parameter description

Parameter	Mandatory	Type	Description
type	Yes	String	• Specifies the EIP type. • The value can be **5_telcom**, **5_union**, **5_bgp**, or **5_sbgp**. – CN South-Guangzhou: **5_bgp** and **5_sbgp** – CN East-Shanghai2: **5_bgp** and **5_sbgp** – CN North-Beijing1: **5_bgp** and **5_sbgp** – CN-Hong Kong: **5_bgp** – CN Southwest-Guiyang1: **5_bgp** and **5_sbgp** – CN North-Beijing4: **5_bgp** and **5_sbgp** • Note: – The configured value must be supported by the system. – **publicip_id** is an IPv4 port. If **publicip_type** is not specified, the default value is **5_bgp**.
ip_version	No	Integer	• Specifies the EIP version. • The value can be **4** and **6**. **4** indicates an IPv4 address, and **6** indicates an IPv6 address. • Note: – The configured value must be supported by the system. – If this parameter is left blank or is an empty string, an IPv4 address is assigned by default.
ip_address	No	String	• Specifies the EIP to be assigned. The system automatically assigns an EIP if you do not specify it. • The value must be a valid IPv4 address in the available IP address range.

Table 10-9 bandwidth parameter description

Parameter	Mandatory	Type	Description
name	No	String	• Specifies the bandwidth name. • The value can contain 1 to 64 characters that can contain letters, digits, underscores (_), hyphens (-), and periods (.). • This parameter is mandatory when **share_type** is set to **PER**. This parameter will be ignored when **share_type** is set to **WHOLE** with an ID specified.

Parameter	Mandatory	Type	Description
size	No	Integer	• Specifies the bandwidth (Mbit/s). • The value ranges from **1** to **300** by default (The specific range may vary depending on the configuration in each region. You can see the bandwidth range of each region on the management console.) • This parameter is mandatory when **share_type** is set to **PER**. This parameter will be ignored when **share_type** is set to **WHOLE** with an ID specified. • The minimum unit for bandwidth adjustment varies depending on the bandwidth range. The details are as follows: – The minimum increment is 1 Mbit/s if the allowed bandwidth ranges from 0 to 300 Mbit/s. – The minimum increment is 50 Mbit/s if the allowed bandwidth ranges from 301 Mbit/s to 1000 Mbit/s. – The minimum increment is 500 Mbit/s if the allowed bandwidth is greater than 1,000 Mbit/s.
id	No	String	• Specifies the bandwidth ID. You can specify an existing shared bandwidth when assigning an EIP. • The value can be the ID of the shared bandwidth whose type is set to **WHOLE**.

Parameter	Mandatory	Type	Description
share_type	Yes	String	• Specifies the bandwidth type. • Value options: – **PER**: indicates dedicated bandwidth. – **WHOLE**: indicated shared bandwidth.
charge_mode	No	String	• The default value is **traffic**. Currently, only billing by traffic is supported.

– Step 1: Apply for an EIP.

```
POST https://{VPCEndpoint}/v1/8b7e35ad379141fc9df3e178bd64f55c/publicips

{
   "publicip": {
      "type": "5_bgp",
      "ip_version": 4
   },
   "bandwidth": {
      "name": "bandwidth123",
      "size": 10,
      "share_type": "PER"
   }
}
```

– Example response

```
{
   "publicip": {
      "id": "f588ccfa-8750-4d7c-bf5d-2ede24414706",
      "status": "PENDING_CREATE",
      "type": "5_bgp",
      "public_ip_address": "139.9.204.183",
      "tenant_id": "8b7e35ad379141fc9df3e178bd64f55c",
      "ip_version": 4,
      "create_time": "2019-06-29 06:45:32",
      "bandwidth_size": 1

   }
}
```

– Step 2: Bind the EIP. (The value of **public_id** is the same as that in the ▪ **Example response**, and the value of **port_id** is the same as that of **vip_port_id** in **Example response 1**.)

```
PUT /v1/8b7e35ad379141fc9df3e178bd64f55c/publicips/f588ccfa-8750-4d7c-bf5d-2ede24414706

{
   "publicip": {
      "port_id": "a7ecbdb5-5a63-41dd-a830-e16c0a7e04a7"
   }
}
```

– Example response

```
{
  "publicip": {
    "id": "f588ccfa-8750-4d7c-bf5d-2ede24414706",
    "status": "ACTIVE",
    "type": "5_bgp",
    "port_id": "a7ecbdb5-5a63-41dd-a830-e16c0a7e04a7",
```



```
    "public_ip_address": "139.9.204.183",
    "private_ip_address": "192.168.1.131",
    "tenant_id": "8b7e35ad379141fc9df3e178bd64f55c",
    "create_time": "2019-06-29 07:33:18",
    "bandwidth_size": 1,
    "ip_version": 4
  }
}
```

- After the preceding steps are complete, the load balancer has the capability of accessing the public network. You can access the load balancer using 139.9.204.183, the value of parameter **public_ip_address**.

Example Response

- Example response 1

```
{
    "loadbalancer": {
        "description": "simple lb",
        "provisioning_status": "ACTIVE",
        "tenant_id": "1867112d054b427e808cc6096d8193a1",
        "project_id": "1867112d054b427e808cc6096d8193a1",
        "created_at": "2019-01-19T05:32:56",
        "admin_state_up": true,
        "updated_at": "2019-01-19T05:32:57",
        "id": "ea2843da-4026-49ec-8338-8fa015b067fc",
        "pools": [],
        "listeners": [],
        "vip_port_id": "a7ecbdb5-5a63-41dd-a830-e16c0a7e04a7",
        "operating_status": "ONLINE",
        "vip_address": "192.168.0.100",
        "vip_subnet_id": "58077bdb-d470-424b-8c45-2e3c65060a5b",
        "provider": "vlb",
        "tags": [],
        "name": "loadbalancer1"
    }
}
```

- Example response 2

```
POST https://{Endpoint}/v2.0/lbaas/loadbalancers

{
    "loadbalancer": {
        "name": "loadbalancer1",
        "description": "simple lb",
        "tenant_id": "1867112d054b427e808cc6096d8193a1",
        "vip_subnet_id": "58077bdb-d470-424b-8c45-2e3c65060a5b",
        "vip_address": "192.168.0.100",
        "admin_state_up": true
    }
}
```

After the preceding steps are complete, the load balancer has the capability of accessing the public network. You can access the load balancer using 139.9.204.183, the value of parameter **public_ip_address**.

Status Code

For details, see **Status Codes**.

10.1.1.2 Querying Load Balancers

Function

This API is used to query load balancers and display them in a list. Filter query and pagination query are supported. Unless otherwise specified, exact match is applied.

Constraints

Parameters **marker**, **limit**, and **page_reverse** are used for pagination query. Parameters **marker** and **page_reverse** take effect only when they are used together with parameter **limit**.

URI

GET /v2.0/lbaas/loadbalancers

Request

Table 10-10 Parameter description

Parameter	Mandatory	Type	Description
marker	No	String	Specifies the ID of the load balancer from which pagination query starts, that is, the ID of the last load balancer on the previous page. This parameter must be used together with **limit**.
limit	No	Integer	Specifies the number of load balancers on each page.
page_reverse	No	Boolean	Specifies the page direction. The value can be **true** or **false**, and the default value is **false**. The last page in the list requested with **page_reverse** set to **false** will not contain the "next" link, and the last page in the list requested with **page_reverse** set to **true** will not contain the "previous" link. This parameter must be used together with **limit**.
tenant_id	No	String	Specifies the ID of the project where the load balancer is used.

Parameter	Mandatory	Type	Description
project_id	No	String	Specifies the ID of the project to which the load balancer belongs. This parameter has the same meaning as **tenant_id**.
id	No	String	Specifies the load balancer ID.
description	No	String	Provides supplementary information about the load balancer. The value contains a maximum of 255 characters.
name	No	String	Specifies the load balancer name. The value contains a maximum of 255 characters.
operating_status	No	String	Specifies the operating status of the load balancer. This parameter is reserved, and its value can be **ONLINE** or **FROZEN**.
provisioning_status	No	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the load balancer.
admin_state_up	No	Boolean	This parameter is reserved, and its value can only be **true**. It specifies the administrative status of the load balancer.
vip_address	No	String	Specifies the private IP address of the load balancer. The value contains a maximum of 64 characters.
vip_port_id	No	String	Specifies the ID of the port bound to the private IP address of the load balancer.
vip_subnet_id	No	String	Specifies the ID of the IPv4 subnet where the load balancer works.
member_address	No	String	Specifies the IP address of the backend server associated with the load balancer.
member_device_id	No	String	Specifies the ID of the cloud server used as the backend server associated with the load balancer.
vpc_id	No	String	Specifies the ID of the VPC where the load balancer works.

Response

Table 10-11 Response parameters

Parameter	Type	Description
loadbalancers	Array	Lists the load balancers. For details, see **Table 10-12**.
loadbalancers_links	Array	Provides links to the previous or next page during pagination query, respectively. This parameter exists only in the response body of pagination query. For details, see **Table 10-15**.

Table 10-12 loadbalancer parameter description

Parameter	Mandatory	Type	Description
name	No	String	Specifies the load balancer name. The value contains a maximum of 255 characters.
description	No	String	Provides supplementary information about the load balancer. The value contains a maximum of 255 characters.
tenant_id	No	String	Specifies the ID of the project where the load balancer is used. The value contains a maximum of 255 characters. The value must be the same as the value of **project_id** in the token.
project_id	No	String	Specifies the ID of the project to which the load balancer belongs. This parameter has the same meaning as **tenant_id**. The value must be the same as the value of **project_id** in the token.

Parameter	Mandatory	Type	Description
vip_subnet_id	Yes	String	Specifies the ID of the IPv4 subnet where the load balancer works. You can obtain the value by calling the API for querying subnets ({VPC endpoint}/v2.0/subnets) using the GET method. The private IP address of the load balancer is in this subnet. Only IPv4 subnets are supported. IPv6 subnets are not supported.
provider	No	String	Specifies the provider of the load balancer. The value can only be **vlb**.
vip_address	No	String	Specifies the private IP address of the load balancer. This IP address must be the one in the subnet specified by **vip_subnet_id**. If this parameter is not specified, an IP address is automatically assigned to the load balancer from the subnet specified by **vip_subnet_id**. The value contains a maximum of 64 characters.
admin_state_up	No	Boolean	Specifies the administrative status of the load balancer. This parameter is reserved. The default value is **true**.

Table 10-13 listeners parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated listener.

Table 10-14 pools parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated backend server group.

Table 10-15 loadbalancers_links parameter description

Parameter	Type	Description
href	String	Provides links to the previous or next page during pagination query, respectively.
rel	String	Specifies the prompt of the previous or next page. The value can be **next** or **previous**. The value **next** indicates the Hypertext Reference (href) containing the URL of the next page, and **previous** indicates the href containing the URL of the previous page.

Example Request

- Example request 1: Querying all load balancers
  ```
  GET https://{Endpoint}/v2.0/lbaas/loadbalancers
  ```
- Example request 2: Querying load balancers by page (Each page contains one load balancer. The ID of the start load balancer is **165b6a38-5278-4569-b747-b2ee65ea84a4**. The load balancer after **165b6a38-5278-4569-b747-b2ee65ea84a4** is the queried load balancer.)
  ```
  GET https://{Endpoint}/v2.0/lbaas/loadbalancers?limit=1&marker=165b6a38-5278-4569-b747-b2ee65ea84a4
  ```
- Example request 3: Querying the load balancer using the IP address of a backend server (192.168.0.191)
  ```
  GET https://{Endpoint}/v2.0/lbaas/loadbalancers?member_address=192.168.0.181
  ```

Example Response

- Example response 1
  ```
  {
     "loadbalancers": [
        {
           "description": "simple lb",
           "admin_state_up": true,
           "tenant_id": "1a3e005cf9ce40308c900bcb08e5320c",
           "project_id": "1a3e005cf9ce40308c900bcb08e5320c",
           "provisioning_status": "ACTIVE",
           "vip_subnet_id": "5328f1e6-ce29-44f1-9493-b128a5653350",
           "listeners": [
              {
                 "id": "45196943-2907-4369-87b1-c009b1d7ac35"
              }
           ],
           "vip_address": "10.0.0.2",
           "vip_port_id": "cbced4fe-6f6f-4fd6-9348-0c3d1219d6ca",
           "provider": "vlb",
           "pools": [
              {
                 "id": "21d49cf7-4fd3-4cb6-8c48-b7fc6c259aab"
           }
           ],
  ```



```
            "id": "a9729389-6147-41a3-ab22-a24aed8692b2",
            "operating_status": "ONLINE",
            "tags": [],
            "name": "loadbalancer1",
            "created_at": "2018-07-25T01:54:13",
            "updated_at": "2018-07-25T01:54:14"
        }
    ]
}
```

- Example response 2

```
{
    "loadbalancers": [
        {
            "description": "",
            "provisioning_status": "ACTIVE",
            "tenant_id": "601240b9c5c94059b63d484c92cfe308",
            "project_id": "601240b9c5c94059b63d484c92cfe308",
            "admin_state_up": true,
            "provider": "vlb",
            "pools": [
                {
                    "id": "b13dba4c-a44c-4c40-8f6e-ce7a162b9f22"
                },
                {
                    "id": "4b9e765f-82ee-4128-911b-0a2d9ebc74c7"
                }
            ],
            "listeners": [
                {
                    "id": "21c41336-d0d3-4349-8641-6e82b4a4d097"
                }
            ],
            "vip_port_id": "44ac5d9b-b0c0-4810-9a9d-c4dbf541e47e",
            "operating_status": "ONLINE",
            "vip_address": "192.168.0.234",
            "vip_subnet_id": "9d60827e-0e5c-490a-8183-0b6ebf9084ca",
            "id": "e79a7dd6-3a38-429a-95f9-c7f78b346cbe",
            "tags": [],
            "name": "elb-robot",
            "created_at": "2018-07-25T01:54:13",
            "updated_at": "2018-07-25T01:54:14"
        }
    ],
    "loadbalancers_links": [
        {
            "href": "https://network.Region.dc1.domainname.com/v2.0/lbaas/loadbalancers?
limit=10&marker=e79a7dd6-3a38-429a-95f9-c7f78b346cbe&page_reverse=True",
            "rel": "previous"
        }
    ]
}
```

- Example response 3

```
{
    "loadbalancers": [
        {
            "description": "",
            "provisioning_status": "ACTIVE",
            "tenant_id": "601240b9c5c94059b63d484c92cfe308",
            "project_id": "601240b9c5c94059b63d484c92cfe308",
            "created_at": "2018-11-29T13:55:20",
            "admin_state_up": true,
            "update_at": "2018-11-29T13:55:21",
            "id": "c1127125-64a9-4394-a08a-ef3be8f7ef9c",
            "pools": [
                {
                    "id": "2f6895be-019b-4c82-9b53-c4a2ac009e20"
                }
            ],
```



```
        "listeners": [
            {
                "id": "5c63d176-444f-4c75-9cfe-bcb8a05a845c"
            }
        ],
        "vip_port_id": "434ac600-b779-4428-b7a7-830e047511f1",
        "operating_status": "ONLINE",
        "vip_address": "192.168.0.181",
        "vip_subnet_id": "9a303536-417c-45dc-a6db-1234b9e1c2b2",
        "provider": "vlb",
        "tags": [],
        "name": "elb-ftci"

    }
  ]
}
```


Status Code

For details, see **Status Codes**.

10.1.1.3 Querying Details of a Load Balancer

Function

This API is used to query details about a load balancer using its ID. You can also query the EIP bound to the load balancer based on the value of **vip_port_id**.

URI

GET /v2.0/lbaas/loadbalancers/{loadbalancer_id}

Table 10-16 Parameter description

Parameter	Mandatory	Type	Description
loadbalancer_id	Yes	String	Specifies the load balancer ID.

Request

None

Response

Table 10-17 Parameter description

Parameter	Type	Description
loadbalancer	Object	Specifies the load balancer. For details, see **Table 10-18**.

Table 10-18 loadbalancer parameter description

Parameter	Mandatory	Type	Description
name	No	String	Specifies the load balancer name. The value contains a maximum of 255 characters.
description	No	String	Provides supplementary information about the load balancer. The value contains a maximum of 255 characters.
provisioning_status	No	String	This parameter is reserved. Specifies the provisioning status of the load balancer. The value can be **ACTIVE**.
tenant_id	No	String	Specifies the ID of the project where the load balancer is used. The value contains a maximum of 255 characters. The value must be the same as the value of **project_id** in the token.
project_id	No	String	Specifies the ID of the project where the load balancer is used. This parameter has the same meaning as **tenant_id**. The value must be the same as the value of **project_id** in the token.
vip_subnet_id	Yes	String	Specifies the ID of the IPv4 subnet where the load balancer works. You can obtain the value by calling the API for querying subnets ({VPC endpoint}/v2.0/subnets) using the GET method. The private IP address of the load balancer is in this subnet. Only IPv4 subnets are supported. IPv6 subnets are not supported.
provider	No	String	Specifies the provider of the load balancer. The value can only be **vlb**.

Parameter	Mandatory	Type	Description
vip_address	No	String	Specifies the private IP address of the load balancer. This IP address must be the one in the subnet specified by **vip_subnet_id**. If this parameter is not specified, an IP address is automatically assigned to the load balancer from the subnet specified by **vip_subnet_id**. The value contains a maximum of 64 characters.
admin_state_up	No	Boolean	Specifies the administrative status of the load balancer. This parameter is reserved. The default value is **true**.

Table 10-19 listeners parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated listener.

Table 10-20 pools parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated backend server group.

Example Request

- Example request 1: Querying details of a load balancer using its ID
- Example request 2: Querying the EIP bound to the load balancer. For details, see **Querying EIPs**.

  ```
  GET https://{EIP_Endpoint}/v1/{project_id}/publicips?port_id={vip_port_id}
  ```

  vip_port_id is the value of **vip_port_id** for the load balancer.

Example Response

- Example response 1

  ```
  {
      "loadbalancer": {
          "description": "",
          "admin_state_up": true,
          "tenant_id": "1867112d054b427e808cc6096d8193a1",
          "project_id": "1867112d054b427e808cc6096d8193a1",
  ```



```
      "provisioning_status": "ACTIVE",
      "vip_subnet_id": "4f5e8efe-fbbe-405e-b48c-a41202ef697c",
      "listeners": [
         {
            "id": "09e64049-2ab0-4763-a8c5-f4207875dc3e"
         }
      ],
      "vip_address": "192.168.2.4",
      "vip_port_id": "c7157e7a-036a-42ca-8474-100be22e3727",
      "provider": "vlb",
      "pools": [
         {
            "id": "b7e53dbd-62ab-4505-a280-5c066078a5c9"
         }
      ],
      "id": "3d77894d-2ffe-4411-ac0a-0d57689779b8",
      "operating_status": "ONLINE",
      "tags": [],
      "name": "lb-2",
      "created_at": "2018-07-25T01:54:13",
      "updated_at": "2018-07-25T01:54:14"
   }
}
```


- Example response 2


```
{
   "publicips": [
      {
         "id": "6285e7be-fd9f-497c-bc2d-dd0bdea6efe0",
         "status": "DOWN",
         "profile": {
           "user_id": "35f2b308f5d64441a6fa7999fbcd4321",
           "product_id": "00301-48027-0--0",
           "region_id": "xxx",
           "order_id": "xxxxxxxxx"
         },
         "type": "5_bgp",
         "public_ip_address": "161.xx.xx.9",
         "private_ip_address": "192.168.2.4",
         "tenant_id": "8b7e35ad379141fc9df3e178bd64f55c",
         "create_time": "2015-07-16 04:22:32",
         "bandwidth_id": "3fa5b383-5a73-4dcb-a314-c6128546d855",
         "bandwidth_share_type": "PER",
         "bandwidth_size": 5,
         "bandwidth_name": "bandwidth-test",
         "enterprise_project_id":"b261ac1f-2489-4bc7-b31b-c33c3346a439",
         "ip_version": 4,
         "port_id": "c7157e7a-036a-42ca-8474-100be22e3727"
      }
   ]
}
```


public_ip_address indicates the EIP bound to the load balancer.

Status Code

For details, see **Status Codes**.

10.1.1.4 Querying the Status Tree of a Load Balancer

Function

This API is used to query the status tree of a load balancer. You can use this API to query details about the associated listeners, backend server groups, backend servers, health checks, forwarding policies, and forwarding rules, helping you understand the topology of resources associated with the load balancer.

URI

GET /v2.0/lbaas/loadbalancers/{loadbalancer_id}/statuses

Table 10-21 Parameter description

Parameter	Mandatory	Type	Description
loadbalancer_id	Yes	String	Specifies the load balancer ID.

Request

None

Response

Table 10-22 Response parameters

Parameter	Type	Description
statuses	Object	Specifies the status tree of a load balancer. For details, see **Table 10-23**.

Table 10-23 statuses parameter description

Parameter	Type	Description
loadbalancer	Object	Specifies the load balancer. For details, see **Table 10-24**.

Table 10-24 loadbalancer parameter description

Parameter	Type	Description
id	String	Specifies the load balancer ID.
name	String	Specifies the load balancer name. The value contains a maximum of 255 characters.
listeners	Array	Lists the listeners added to the load balancer. For details of this parameter, see **Table 10-25**.

Parameter	Type	Description
pools	Array	Lists the backend server groups associated with the load balancer. For details of this parameter, see **Table 10-26**.
operating_status	String	This field is reserved. It specifies the operating status of the load balancer. The value can be one of the following: • **ONLINE** (default): The load balancer is running normally. • **DEGRADED**: This status is displayed only when **provisioning_status** of a forwarding policy or forwarding rule added to a listener of the load balancer is set to **ERROR** and the API for querying the load balancer status tree is called. • **DISABLED**: This status is displayed only when **admin_state_up** of the load balancer is set to **false** and the API for querying the load balancer status tree is called. • **FROZEN**: The load balancer is frozen.
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the load balancer.

Table 10-25 listeners parameter description

Parameter	Type	Description
id	String	Specifies the listener ID.
name	String	Specifies the listener name.
l7policies	Array	Lists associated forwarding policies. For details of this parameter, see **Table 10-29**.

Parameter	Type	Description
pools	Array	Lists the backend server groups associated with the listener. For details of this parameter, see **Table 10-26**.
operating_status	String	This parameter is reserved, and its value can only be **ONLINE**. It specifies the operating status of the listener.
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the listener.

Table 10-26 pools parameter description

Parameter	Type	Description
id	String	Specifies the ID of the backend server group.
name	String	Specifies the name of the backend server group.
healthmonitor	Object	Provides health check details of the backend server group. For details of this parameter, see **Table 10-27**.
members	Array	Lists the members contained in the backend server group. For details of this parameter, see **Table 10-28**.
operating_status	String	This parameter is reserved, and its value can only be **ONLINE**. It specifies the operating status of the backend server group.
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the backend server group.

Table 10-27 healthmonitor parameter description

Parameter	Type	Description
id	String	Specifies the health check ID.
name	String	Specifies the health check name.
type	String	• Specifies the health check protocol. • The value can be **UDP_CONNECT**, **TCP**, or **HTTP**.
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the health check.

Table 10-28 members parameter description

Parameter	Type	Description
id	String	Specifies the backend server ID.
address	String	Specifies the private IP address of the backend server, for example, 192.168.3.11.
protocol_port	Integer	Specifies the port used by the backend server. The port number ranges from 0 to 65535.

Parameter	Type	Description
operating_status	String	This parameter is reserved. It specifies the operating status of the backend server. The value can be one of the following: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group that the backend server belongs to. • **DISABLED**: The backend server is not available. This status is displayed only when **admin_state_up** of the backend server, or the backend server group to which it belongs, or the associated load balancer is set to **false** and the API for querying the load balancer status tree is called. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist. **NOTE** When **admin_state_up** is set to **false** and **operating_status** is set to **OFFLINE** for a backend server, **DISABLED** is returned for **operating_status** of the backend server in the response of this API.
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the backend server.

Table 10-29 l7policies parameter description

Parameter	Type	Description
id	String	Specifies the forwarding policy ID.
name	String	Specifies the forwarding policy name.

Parameter	Type	Description
rules	Array	Lists the forwarding rules of the forwarding policy. For details of this parameter, see **Table 10-30**.
action	String	• Specifies whether requests are forwarded to another backend server group or redirected to an HTTPS listener. • The value can be **REDIRECT_TO_POOL** or **REDIRECT_TO_LISTENER**. – **REDIRECT_TO_POOL**: Requests are forwarded to another backend server group. – **REDIRECT_TO_LISTENER**: Requests are redirected to an HTTPS listener.
provisioning_status	String	This parameter is reserved. It specifies the provisioning status of the forwarding policy. Value options: • **ACTIVE** (default): The forwarding policy is normal. • **ERROR**: Another forwarding policy of the same listener has the same forwarding rule.

Table 10-30 rules parameter description

Parameter	Type	Description
id	String	Specifies the forwarding rule ID.
type	String	• Specifies the match type of a forwarding rule. • The value can be **PATH** or **HOST_NAME**. – **PATH**: matches the path in the request. – **HOST_NAME**: matches the domain name in the request.

Parameter	Type	Description
provisioning_status	String	This parameter is reserved. It specifies the provisioning status of the forwarding rule. The value can be one of the following: • **ACTIVE** (default): The forwarding rule is normal. • **ERROR**: Another forwarding policy of the same listener has the same forwarding rule.

Example Request

- Example request
  GET https://{Endpoint}/v2.0/lbaas/loadbalancers/38278031-cfca-44be-81be-a412f618773b/statuses

Example Response

- Example response

```
{
   "statuses": {
      "loadbalancer": {
         "name": "lb-jy",
         "provisioning_status": "ACTIVE",
         "listeners": [
            {
               "name": "listener-jy-1",
               "provisioning_status": "ACTIVE",
               "pools": [
                  {
                     "name": "pool-jy-1",
                     "provisioning_status": "ACTIVE",
                     "healthmonitor": {
                        "type": "TCP",
                        "id": "7422b51a-0ed2-4702-9429-4f88349276c6",
                        "name": "",
                        "provisioning_status": "ACTIVE"
                     },
                     "members": [
                        {
                           "protocol_port": 80,
                           "address": "192.168.44.11",
                           "id": "7bbf7151-0dce-4087-b316-06c7fa17b894",
                           "operating_status": "ONLINE",
                           "provisioning_status": "ACTIVE"
                        }
                     ],
                     "id": "c54b3286-2349-4c5c-ade1-e6bb0b26ad18",
                     "operating_status": "ONLINE"
                  }
               ],
               "l7policies": [],
               "id": "eb84c5b4-9bc5-4bee-939d-3900fb05dc7b",
               "operating_status": "ONLINE"
            }
         ],
         "pools": [
```

```
            {
                "name": "pool-jy-1",
                "provisioning_status": "ACTIVE",
                "healthmonitor": {
                    "type": "TCP",
                    "id": "7422b51a-0ed2-4702-9429-4f88349276c6",
                    "name": "",
                    "provisioning_status": "ACTIVE"
                },
                "members": [
                    {
                        "protocol_port": 80,
                        "address": "192.168.44.11",
                        "id": "7bbf7151-0dce-4087-b316-06c7fa17b894",
                        "operating_status": "ONLINE",
                        "provisioning_status": "ACTIVE"
                    }
                ],
                "id": "c54b3286-2349-4c5c-ade1-e6bb0b26ad18",
                "operating_status": "ONLINE"
            }
        ],
        "id": "38278031-cfca-44be-81be-a412f618773b",
        "operating_status": "ONLINE"
    }
  }
}
```


Status Code

For details, see **Status Codes**.

10.1.1.5 Updating a Load Balancer

Function

This API is used to update the name or description of a load balancer.

URI

PUT /v2.0/lbaas/loadbalancers/{loadbalancer_id}

Table 10-31 Parameter description

Parameter	Mandatory	Type	Description
loadbalancer_id	Yes	String	Specifies the load balancer ID.

Request

Table 10-32 Parameter description

Parameter	Mandatory	Type	Description
loadbalancer	Yes	Object	Specifies the load balancer. For details, see **Table 10-33**.

Table 10-33 loadbalancer parameter description

Parameter	Mandatory	Type	Description
name	No	String	Specifies the load balancer name. The value contains a maximum of 255 characters.
description	No	String	Provides supplementary information about the load balancer. The value contains a maximum of 255 characters.
admin_state_up	No	Boolean	Specifies the administrative status of the load balancer. This parameter is reserved. The default value is **true**.

Response

Table 10-34 Response parameters

Parameter	Type	Description
loadbalancer	Object	Specifies the load balancer. For details, see **Table 10-35**.

Table 10-35 loadbalancer parameter description

Parameter	Type	Description
id	String	Specifies the load balancer ID.
project_id	String	Specifies the ID of the project to which the load balancer belongs. This parameter has the same meaning as **tenant_id**.

Parameter	Type	Description
tenant_id	String	Specifies the ID of the project where the load balancer is used. The value contains a maximum of 255 characters.
name	String	Specifies the load balancer name. The value contains a maximum of 255 characters.
description	String	Provides supplementary information about the load balancer. The value contains a maximum of 255 characters.
vip_subnet_id	String	Specifies the ID of the IPv4 subnet where the load balancer works.
vip_port_id	String	Specifies the ID of the port bound to the private IP address of the load balancer. When you create a load balancer, the system automatically creates a port and associates it with a security group. However, the security group will not take effect.
provider	String	Specifies the provider of the load balancer.
vip_address	String	Specifies the private IP address of the load balancer. The value contains a maximum of 64 characters.
listeners	Array	Lists the IDs of listeners added to the load balancer. For details, see **Table 10-5**.
pools	Array	Lists the IDs of backend server groups associated with the load balancer. For details, see **Table 10-6**.

Parameter	Type	Description
operating_status	String	Specifies the operating status of the load balancer. This parameter is reserved, and its value can be **ONLINE** or **FROZEN**.
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the load balancer.
admin_state_up	Boolean	Specifies the administrative status of the load balancer. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
tags	Array	Lists load balancer tags.
created_at	String	Specifies the time when the load balancer was created. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format. The value contains a maximum of 19 characters.
updated_at	String	Specifies the time when the load balancer was updated. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format. The value contains a maximum of 19 characters.

Table 10-36 listeners parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated listener.

Table 10-37 pools parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated backend server group.

Example Request

- Example request: Modifying the load balancer name and description

```
PUT https://{Endpoint}/v2.0/lbaas/loadbalancers/1e11b74e-30b7-4b78-b09b-84aec4a04487

{
   "loadbalancer": {
      "name": "lb_update_test",
      "description": "lb update test"
   }
}
```

Example Response

- Example response

```
{
  "loadbalancer": {
    "description": "simple lb2",
    "admin_state_up": true,
    "tenant_id": "145483a5107745e9b3d80f956713e6a3",
    "project_id": "145483a5107745e9b3d80f956713e6a3",
    "provisioning_status": "ACTIVE",
    "vip_subnet_id": "823d5866-6e30-45c2-9b1a-a1ebc3757fdb",
    "listeners": [
      {
        "id": "37ffe679-08ef-436e-b6bd-cf66fb4c3de2"
      }
    ],
    "vip_address": "192.172.1.68",
    "vip_port_id": "f42e3019-67f7-4d2a-8d1c-af49e7c22fa6",
    "tags": [],
    "provider": "vlb",
    "pools": [
      {
        "id": "75c4f2d4-a213-4408-9fa8-d64708e8d1df"
      }
    ],
    "id": "c32a9f9a-0cc6-4f38-bb9c-cde79a533c19",
    "operating_status": "ONLINE",
    "name": "loadbalancer-test2",
    "created_at": "2018-07-25T01:54:13",
    "updated_at": "2018-07-25T01:54:14"
  }
}
```

Status Code

For details, see **Status Codes**.

10.1.1.6 Deleting a Load Balancer

Function

This API is used to delete a specific load balancer.

Constraints

All listeners added to the load balancer must be deleted before the load balancer is deleted.

URI

DELETE /v2.0/lbaas/loadbalancers/{loadbalancer_id}

Table 10-38 Parameter description

Parameter	Mandatory	Type	Description
loadbalancer_id	Yes	String	Specifies the load balancer ID.
cascade	No	Boolean	**[Discarded]** Specifies whether to delete the resources associated with the load balancer when the load balancer is deleted, including the listeners, backend server groups, and backend servers.

Request

None

Response

None

Example Request

Example request: Deleting a load balancer

```
DELETE https://{endpoint}/v2.0/lbaas/loadbalancers/90f7c765-0bc9-47c4-8513-4cc0c264c8f8
```

Example Response

Example response

None

Status Code

For details, see **Status Codes**.

10.1.2 Listener

10.1.2.1 Adding a Listener

Function

This API is used to add a listener to a load balancer.

URI

POST /v2.0/lbaas/listeners

Request

Table 10-39 Parameter description

Parameter	Mandatory	Type	Description
listener	Yes	Object	Specifies the listener. For details, see **Table 10-40**.

Table 10-40 listener parameter description

Parameter	Mandatory	Type	Description
tenant_id	No	String	Specifies the ID of the project where the listener is used. The value must be the same as the value of **project_id** in the token. The value contains a maximum of 255 characters.
project_id	No	String	Specifies the ID of the project to which the listener belongs. This parameter has the same meaning as **tenant_id**. The value must be the same as the value of **project_id** in the token.
name	No	String	Specifies the listener name. The value contains a maximum of 255 characters.
description	No	String	Provides supplementary information about the listener. The value contains a maximum of 255 characters.
protocol	Yes	String	Specifies the protocol used by the listener. The value can be **TCP**, **HTTP**, **UDP**, or **TERMINATED_HTTPS**.

Parameter	Mandatory	Type	Description
protocol_port	Yes	Integer	Specifies the port used by the listener. The port number ranges from 1 to 65535. **NOTE** If the protocol used by the listener is UDP, the port number cannot be 4789.
loadbalancer_id	Yes	String	Specifies the ID of the associated load balancer.
connection_limit	No	Integer	Specifies the maximum number of connections. The value ranges from **-1** to **2147483647**. The default value is **-1**, indicating that there is no restriction on the maximum number of connections. This parameter is reserved.
admin_state_up	No	Boolean	Specifies the administrative status of the listener. This parameter is reserved, and the default value is **true**.
http2_enable	No	Boolean	Specifies whether to use HTTP/2. The value can be **true** or **false**. ● **true**: HTTP/2 is used. ● **false**: HTTP/2 is not used. The default value is **false**. This parameter is valid only when the protocol used by the listener is set to **TERMINATED_HTTPS**.

Parameter	Mandatory	Type	Description
default_pool_id	No	String	Specifies the ID of the associated backend server group. If a request does not match the forwarding policy, the request is forwarded to the default backend server group for processing. If the value is **null**, the listener has no default backend server group. This parameter has the following constraints: ● Its value cannot be the ID of any backend server group of other listeners. ● Its value cannot be the ID of any backend server group associated with the forwarding policies set for other listeners. The relationships between the protocol used by the listener and the protocol of the backend server group are as follows: ● When the protocol used by the listener is **TCP**, the protocol of the backend server group must be **TCP**. ● When the protocol used by the listener is **UDP**, the protocol of the backend server group must be **UDP**. ● When the protocol used by the listener is **HTTP** or **TERMINATED_HTTPS**, the protocol of the backend server group must be **HTTP**.

Parameter	Mandatory	Type	Description
default_tls_container_ref	No	String	Specifies the ID of the server certificate used by the listener. This parameter is mandatory when **protocol** is set to **TERMINATED_HTTPS**. The default value is **null** when **protocol** is not set to **TERMINATED_HTTPS**. The value contains a maximum of 128 characters. **NOTE** This parameter is valid only when **protocol** is set to **TERMINATED_HTTPS**.
client_ca_tls_container_ref	No	String	Specifies the ID of the CA certificate used by the listener. The default value is **null**. The value contains a maximum of 128 characters. **NOTE** This parameter is valid only when **protocol** is set to **TERMINATED_HTTPS**.
sni_container_refs	No	Array	Lists the IDs of SNI certificates (server certificates with domain names) used by the listener. If the parameter value is an empty list, the SNI feature is disabled. The default value is **[]**. **NOTE** This parameter is valid only when **protocol** is set to **TERMINATED_HTTPS**.
tls_ciphers_policy	No	String	Specifies the security policy used by the listener. This parameter is valid only when the protocol used by the listener is set to **TERMINATED_HTTPS**. The value can be **tls-1-0-inherit**, **tls-1-0**, **tls-1-1**, **tls-1-2**, or **tls-1-2-strict**, and the default value is **tls-1-0**. For details of cipher suites for each security policy, see **Table 10-41**.

Table 10-41 tls_ciphers_policy parameter description

Security Policy	TLS Version	Cipher Suite
tls-1-0-inherit	TLS 1.2 TLS 1.1 TLS 1.0	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:DHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:AES128-SHA:AES256-SHA:DHE-DSS-AES128-SHA:CAMELLIA128-SHA:EDH-RSA-DES-CBC3-SHA:DES-CBC3-SHA:ECDHE-RSA-RC4-SHA:RC4-SHA:DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:DHE-RSA-CAMELLIA256-SHA:DHE-DSS-CAMELLIA256-SHA:CAMELLIA256-SHA:EDH-DSS-DES-CBC3-SHA:DHE-RSA-CAMELLIA128-SHA:DHE-DSS-CAMELLIA128-SHA
tls-1-0	TLS 1.2 TLS 1.1 TLS 1.0	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:AES128-SHA:AES256-SHA
tls-1-1	TLS 1.2 TLS 1.1	
tls-1-2	TLS 1.2	
tls-1-2-strict	TLS 1.2	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384

Response

Table 10-42 Response parameters

Parameter	Type	Description
listener	Object	Specifies the listener. For details, see **Table 10-43**.

Table 10-43 listeners parameter description

Parameter	Type	Description
id	String	Specifies the listener ID.
tenant_id	String	Specifies the ID of the project where the listener is used.
project_id	String	Specifies the ID of the project to which the listener belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the listener name.
description	String	Provides supplementary information about the listener.
protocol	String	Specifies the protocol used by the listener. The value can be **TCP**, **HTTP**, **UDP**, or **TERMINATED_HTTPS**.
protocol_port	Integer	Specifies the port used by the listener. The port number ranges from 1 to 65535.
loadbalancers	Array	Specifies the ID of the associated load balancer. For details, see **Table 10-44**.
connection_limit	Integer	Specifies the maximum number of connections. The value ranges from **-1** to **2147483647**. The default value is **-1**, indicating that there is no restriction on the maximum number of connections. This parameter is reserved.
admin_state_up	Boolean	Specifies the administrative status of the listener. This parameter is reserved. The value can be **true** or **false**. • **true**: The load balancer is enabled. • **false**: The load balancer is disabled.

Parameter	Type	Description
http2_enable	Boolean	Specifies whether to use HTTP/2. The value can be **true** or **false**. • **true**: HTTP/2 is used. • **false**: HTTP/2 is not used. This parameter is valid only when the protocol used by the listener is set to **TERMINATED_HTTPS**.
default_pool_id	String	Specifies the ID of the associated backend server group. If a request does not match the forwarding policy, the request is forwarded to the default backend server group for processing. If the value is **null**, the listener has no default backend server group.
default_tls_container_ref	String	Specifies the ID of the server certificate used by the listener. For details, see **Certificate**. This parameter is mandatory when **protocol** is set to **TERMINATED_HTTPS**.
client_ca_tls_container_ref	String	Specifies the ID of the CA certificate used by the listener. For details, see **Certificate**.
sni_container_refs	Array	Lists the IDs of SNI certificates (server certificates with domain names) used by the listener. If the parameter value is an empty list, the SNI feature is disabled.
tags	Array	Tags the listener.
created_at	String	Specifies the time when the listener was created. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format.
updated_at	String	Specifies the time when the listener was updated. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format.
tls_ciphers_policy	String	Specifies the security policy used by the listener. This parameter is valid only when the protocol used by the listener is set to **TERMINATED_HTTPS**. The value can be **tls-1-0-inherit**, **tls-1-0**, **tls-1-1**, **tls-1-2**, or **tls-1-2-strict**, and the default value is **tls-1-0**. For details of cipher suites for each security policy, see **Table 10-41**.

Table 10-44 loadbalancers parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated load balancer.

Example Request

- Example request 1: Adding a TCP listener

```
POST https://{Endpoint}/v2.0/lbaas/listeners

{
   "listener": {
      "protocol_port": 80,
      "protocol": "TCP",
      "loadbalancer_id": "0416b6f1-877f-4a51-987e-978b3f084253",
      "name": "listener-test",
      "admin_state_up": true
   }
}
```

- Example request 2: Adding an HTTPS listener

```
POST https://{Endpoint}/v2.0/lbaas/listeners

{
   "listener": {
      "protocol_port": 25,
      "protocol": "TERMINATED_HTTPS",
      "default_tls_container_ref": "02dcd56799e045bf8b131533cc911dd6",
      "loadbalancer_id": "0416b6f1-877f-4a51-987e-978b3f084253",
      "name": "listener-test",
      "admin_state_up": true

   }
}
```

Example Response

- Example response 1

```
{
   "listener": {
      "protocol_port": 80,
      "protocol": "TCP",
      "description": "",
      "client_ca_tls_container_ref": null,
      "default_tls_container_ref": null,
      "admin_state_up": true,
      "http2_enable": false,
      "loadbalancers": [
         {
            "id": "0416b6f1-877f-4a51-987e-978b3f084253"
         }
      ],
      "tenant_id": "145483a5107745e9b3d80f956713e6a3",
      "project_id": "145483a5107745e9b3d80f956713e6a3",
      "sni_container_refs": [],
      "connection_limit": -1,
      "default_pool_id": null,
      "tags": [],
      "id": "b7f32b52-6f17-4b16-9ec8-063d71b653ce",
      "name": "listener-test",
      "created_at": "2018-07-25T01:54:13",
      "updated_at": "2018-07-25T01:54:14"
```



```
    }
}
```

- Example response 2

```
{
    "listener": {
        "protocol_port": 25,
        "protocol": "TERMINATED_HTTPS",
        "description": "",
        "default_tls_container_ref": "02dcd56799e045bf8b131533cc911dd6",
        "sni_container_refs": [],
        "loadbalancers": [
            {
                "id": "0416b6f1-877f-4a51-987e-978b3f084253"
            }
        ],
        "tenant_id": "601240b9c5c94059b63d484c92cfe308",
        "project_id": "601240b9c5c94059b63d484c92cfe308",
        "created_at": "2019-01-21T12:38:31",
        "client_ca_tls_container_ref": null,
        "connection_limit": -1,
        "updated_at": "2019-01-21T12:38:31",
        "http2_enable": false,
        "admin_state_up": true,
        "default_pool_id": null,
        "id": "b56634cd-5ba8-460e-b5a2-6de5ba8eaf60",
        "tags": [],
        "name": "listener-test"

    }
}
```

Status Code

For details, see **Status Codes**.

10.1.2.2 Querying Listeners

Function

This API is used to query the listeners and display them in a list. Filter query and pagination query are supported. Unless otherwise specified, exact match is applied.

You can query listeners using information such as listener ID, protocol used by the listener, port used by the listener, or backend server private IP address.

Constraints

Parameters **marker**, **limit**, and **page_reverse** are used for pagination query. Parameters **marker** and **page_reverse** take effect only when they are used together with parameter **limit**.

URI

GET /v2.0/lbaas/listeners

Request

Table 10-45 Parameter description

Parameter	Mandatory	Type	Description
marker	No	String	Specifies the ID of the listener from which pagination query starts, that is, the ID of the last listener on the previous page. This parameter must be used together with **limit**.
limit	No	Integer	Specifies the number of listeners on each page.
page_reverse	No	Boolean	Specifies the page direction. The value can be **true** or **false**, and the default value is **false**. The last page in the list requested with **page_reverse** set to **false** will not contain the "next" link, and the last page in the list requested with **page_reverse** set to **true** will not contain the "previous" link. This parameter must be used together with **limit**.
id	No	String	Specifies the listener ID.
tenant_id	No	String	Specifies the ID of the project where the listener is used.
project_id	No	String	Specifies the ID of the project to which the listener belongs. This parameter has the same meaning as **tenant_id**.
name	No	String	Specifies the listener name. The value contains a maximum of 255 characters.
description	No	String	Provides supplementary information about the listener. The value contains a maximum of 255 characters.
loadbalancer_id	No	String	Specifies the ID of the associated load balancer.

Parameter	Mandatory	Type	Description
connection_limit	No	Integer	Specifies the maximum number of connections.
admin_state_up	No	Boolean	Specifies the administrative status of the listener. This parameter is reserved, and the default value is **true**.
default_pool_id	No	String	Specifies the ID of the associated backend server group.
http2_enable	No	Boolean	Specifies whether to use HTTP/2. The value can be **true** or **false**. • **true**: HTTP/2 is used. • **false**: HTTP/2 is not used.
default_tls_container_ref	No	String	Specifies the ID of the server certificate used by the listener. The value contains a maximum of 128 characters.
client_ca_tls_container_ref	No	String	Specifies the ID of the CA certificate used by the listener. The value contains a maximum of 128 characters.
protocol	No	String	Specifies the protocol used by the listener. The value can be **TCP**, **HTTP**, **UDP**, or **TERMINATED_HTTPS**.
protocol_port	No	Integer	Specifies the port used by the listener.
tls_ciphers_policy	No	String	Specifies the security policy used by the listener. This parameter is valid only when the protocol used by the listener is set to **TERMINATED_HTTPS**. The value can be **tls-1-0**, **tls-1-1**, **tls-1-2**, or **tls-1-2-strict**. For details of cipher suites for each security policy, see **Table 10-46**.
tls_container_id	No	String	Queries the listener associated with the certificate.

Parameter	Mandatory	Type	Description
sni_container_refs	No	String	Queries the listener associated with the SNI certificate.

Table 10-46 tls_ciphers_policy parameter description

Security Policy	TLS Version	Cipher Suite
tls-1-0-inherit	TLS 1.2 TLS 1.1 TLS 1.0	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:DHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:AES128-SHA:AES256-SHA:DHE-DSS-AES128-SHA:CAMELLIA128-SHA:EDH-RSA-DES-CBC3-SHA:DES-CBC3-SHA:ECDHE-RSA-RC4-SHA:RC4-SHA:DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:DHE-RSA-CAMELLIA256-SHA:DHE-DSS-CAMELLIA256-SHA:CAMELLIA256-SHA:EDH-DSS-DES-CBC3-SHA:DHE-RSA-CAMELLIA128-SHA:DHE-DSS-CAMELLIA128-SHA
tls-1-0	TLS 1.2 TLS 1.1 TLS 1.0	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:AES128-SHA:AES256-SHA
tls-1-1	TLS 1.2 TLS 1.1	
tls-1-2	TLS 1.2	
tls-1-2-strict	TLS 1.2	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384

Response

Table 10-47 Parameter description

Parameter	Type	Description
listeners	Array	Lists the listeners. For details, see **Table 10-48**.
listeners_links	Array	Provides links to the previous or next page during pagination query, respectively. This parameter exists only in the response body of pagination query. For details, see **Table 10-51**.

Table 10-48 listeners parameter description

Parameter	Type	Description
id	String	Specifies the listener ID.
tenant_id	String	Specifies the ID of the project where the listener is used. The value contains a maximum of 255 characters.
project_id	String	Specifies the ID of the project to which the listener belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the listener name. The value contains a maximum of 255 characters.
description	String	Provides supplementary information about the listener. The value contains a maximum of 255 characters.
protocol	String	Specifies the protocol used by the listener. The value can be **TCP**, **HTTP**, **UDP**, or **TERMINATED_HTTPS**.
protocol_port	Integer	Specifies the port used by the listener. The port number ranges from 1 to 65535.
loadbalancers	Array	Specifies the ID of the associated load balancer.

Parameter	Type	Description
connection_limit	Integer	Specifies the maximum number of connections. The value ranges from **-1** to **2147483647**. **NOTE** This parameter is reserved. The default value is **-1**, indicating that there is no restriction on the maximum number of connections.
admin_state_up	Boolean	Specifies the administrative status of the listener. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
http2_enable	Boolean	Specifies whether to use HTTP/2. The value can be **true** or **false**. • **true**: HTTP/2 will be used. • **false**: HTTP/2 will not be used. **NOTE** This parameter is valid only when the protocol used by the listener is set to **TERMINATED_HTTPS**.
keepalive_timeout	Integer	Specifies the idle timeout duration in the unit of second. This parameter applies only to TCP, HTTP, or HTTPS listeners. The value can be one of the following: • TCP listeners: The value ranges from **10** to **4000**, and the default value is **300**. • HTTP or HTTPS listeners: The value ranges from **0** to **4000**, and the default value is **60**.

Parameter	Type	Description
client_timeout	Integer	Specifies the request timeout duration in the unit of second. The value ranges from **1** to **300**. The default value is **60**. This parameter is valid only when **protocol** is set to **HTTP** or **HTTPS**. In other cases, the request body does not contain this parameter. Otherwise, an error is reported. When **protocol** is set to **HTTP** or **HTTPS**, if the request body does not contain this parameter or the value of this parameter is **null**, the default value is used.
member_timeout	Integer	Specifies the response timeout duration in the unit of second. The value ranges from **1** to **300**. The default value is **60**. This parameter is valid only when **protocol** is set to **HTTP** or **HTTPS**. In other cases, the request body does not contain this parameter. Otherwise, an error is reported. When **protocol** is set to **HTTP** or **HTTPS**, if the request body does not contain this parameter or the value of this parameter is **null**, the default value is used.
default_pool_id	String	Specifies the ID of the associated backend server group. **NOTE** If a request does not match the forwarding policy, the request is forwarded to the default backend server group for processing. If the value is **null**, the listener has no default backend server group.
default_tls_container_ref	String	Specifies the ID of the server certificate used by the listener. This parameter is mandatory when **protocol** is set to **TERMINATED_HTTPS**. The value contains a maximum of 128 characters.

Parameter	Type	Description
client_ca_tls_container_ref	String	Specifies the ID of the CA certificate used by the listener. The value contains a maximum of 128 characters.
sni_container_refs	Array	Lists the IDs of SNI certificates (server certificates with domain names) used by the listener.
tags	Array	Tags the listener.
created_at	String	Specifies the time when the listener was created. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format. The value contains a maximum of 19 characters.
updated_at	String	Specifies the time when the listener was updated. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format. The value contains a maximum of 19 characters.
listeners_links	Array	Provides links to the previous or next page during pagination query, respectively. This parameter exists only in the response body of pagination query.
tls_ciphers_policy	String	Specifies the security policy used by the listener. This parameter is valid only when the protocol used by the listener is set to **TERMINATED_HTTPS**. The value can be **tls-1-0-inherit**, **tls-1-0**, **tls-1-1**, **tls-1-2**, or **tls-1-2-strict**, and the default value is **tls-1-0**. For details of cipher suites for each security policy, see **Table 10-50**.

Table 10-49 loadbalancers parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated load balancer.

Table 10-50 tls_ciphers_policy parameter description

Security Policy	TLS Version	Cipher Suite
tls-1-0-inherit	TLS 1.2 TLS 1.1 TLS 1.0	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:DHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:AES128-SHA:AES256-SHA:DHE-DSS-AES128-SHA:CAMELLIA128-SHA:EDH-RSA-DES-CBC3-SHA:DES-CBC3-SHA:ECDHE-RSA-RC4-SHA:RC4-SHA:DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:DHE-RSA-CAMELLIA256-SHA:DHE-DSS-CAMELLIA256-SHA:CAMELLIA256-SHA:EDH-DSS-DES-CBC3-SHA:DHE-RSA-CAMELLIA128-SHA:DHE-DSS-CAMELLIA128-SHA
tls-1-0	TLS 1.2 TLS 1.1 TLS 1.0	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:AES128-SHA:AES256-SHA
tls-1-1	TLS 1.2 TLS 1.1	
tls-1-2	TLS 1.2	
tls-1-2-strict	TLS 1.2	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384

Table 10-51 listeners_links parameter description

Parameter	Type	Description
href	String	Provides links to the previous or next page during pagination query, respectively.
rel	String	Specifies the prompt of the previous or next page. The value can be **next** or **previous**. The value **next** indicates the href containing the URL of the next page, and **previous** indicates the href containing the URL of the previous page.

Example Request

- Example request 1: Querying all listeners
  ```
  GET https://{Endpoint}/v2.0/lbaas/listeners?limit=2
  ```
- Request example 2: Querying UDP listeners
  ```
  GET https://{Endpoint}/v2.0/lbaas/listeners?protocol=UDP
  ```

Example Response

- Example response 1
  ```
  {
     "listeners": [
        {
           "client_ca_tls_container_ref": null,
           "protocol": "TCP",
           "description": "",
           "default_tls_container_ref": null,
           "admin_state_up": true,
           "http2_enable": false,
           "loadbalancers": [
              {
                 "id": "bc7ba445-035a-4464-a1a3-a62cf4a14116"
              }
           ],
           "tenant_id": "601240b9c5c94059b63d484c92cfe308",
           "project_id": "601240b9c5c94059b63d484c92cfe308",
           "sni_container_refs": [],
           "connection_limit": -1,
           "protocol_port": 80,
           "default_pool_id": "ed75f16e-fcc6-403e-a3fb-4eae82005eab",
           "id": "75045172-70e9-480d-9443-b8b6459948f7",
           "tags": [],
           "name": "listener-cb2n",

           "created_at": "2018-07-25T01:54:13",
           "updated_at": "2018-07-25T01:54:14"
        },
        {
           "client_ca_tls_container_ref": null,
           "protocol": "TCP",
           "description": "",
           "default_tls_container_ref": null,
  ```



```
            "admin_state_up": true,
            "http2_enable": false,
            "loadbalancers": [
               {
                  "id": "165b6a38-5278-4569-b747-b2ee65ea84a4"
               }
            ],
            "tenant_id": "601240b9c5c94059b63d484c92cfe308",
            "project_id": "601240b9c5c94059b63d484c92cfe308",
            "sni_container_refs": [],
            "connection_limit": -1,
            "protocol_port": 8080,
            "default_pool_id": null,
            "id": "dada0003-7b0e-4de8-a4e1-1e937be2ba14",
            "tags": [],
            "name": "lsnr_name_mod",
            "created_at": "2018-07-25T01:54:13",
            "updated_at": "2018-07-25T01:54:14"

,

         }
      ],
      "listeners_links": [
         {
         "href": "https://{Endpoint}/v2.0/lbaas/listeners?limit=2&marker=042cc6a5-
e385-4e39-83de-4dde1f801ccb",
         "rel": "next"
         },
         {
         "href": "https://{Endpoint}/v2.0/lbaas/listeners?limit=2&marker=025fcaa9-0159-4a0d-8583-
d97fa77d9972&page_reverse=True",
         "rel": "previous"
         }
      ]
}
```


- Example response 2


```
{
   "listeners": [
      {
         "protocol_port": 64809,
         "protocol": "UDP",
         "description": "",
         "default_tls_container_ref": null,
         "sni_container_refs": [],
         "loadbalancers": [
            {
               "id": "c1127125-64a9-4394-a08a-ef3be8f7ef9c"
            }
         ],
         "tenant_id": "601240b9c5c94059b63d484c92cfe308",
         "project_id": "601240b9c5c94059b63d484c92cfe308",
         "created_at": "2018-11-29T13:56:21",
         "client_ca_tls_container_ref": null,
         "connection_limit": -1,
         "updated_at": "2018-11-29T13:56:22",
         "http2_enable": false,

         "admin_state_up": true,
         "default_pool_id": "2f6895be-019b-4c82-9b53-c4a2ac009e20",
         "id": "5c63d176-444f-4c75-9cfe-bcb8a05a845c",
         "tags": [],
         "name": "listener-tvp8"
      }
   ]
}
```


Status Code

For details, see **Status Codes**.

10.1.2.3 Querying Details of a Listener

Function

This API is used to query details about a listener using its ID.

URI

GET /v2.0/lbaas/listeners/{listener_id}

Table 10-52 Parameter description

Parameter	Mandatory	Type	Description
listener_id	Yes	String	Specifies the listener ID.

Request

None

Response

Table 10-53 Response parameters

Parameter	Type	Description
listener	Object	Lists the listeners. For details, see **Table 10-54**.

Table 10-54 listeners parameter description

Parameter	Type	Description
id	String	Specifies the listener ID.
tenant_id	String	Specifies the ID of the project where the listener is used.
project_id	String	Specifies the ID of the project to which the listener belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the listener name.
description	String	Provides supplementary information about the listener.

Parameter	Type	Description
protocol	String	Specifies the protocol used by the listener. The value can be **TCP**, **HTTP**, **UDP**, or **TERMINATED_HTTPS**.
protocol_port	Integer	Specifies the port used by the listener. The port number ranges from 1 to 65535.
loadbalancers	Array	Specifies the ID of the associated load balancer. For details, see **Table 10-44**.
connection_limit	Integer	Specifies the maximum number of connections. The value ranges from **-1** to **2147483647**. The default value is **-1**, indicating that there is no restriction on the maximum number of connections. This parameter is reserved.
admin_state_up	Boolean	Specifies the administrative status of the listener. This parameter is reserved. The value can be **true** or **false**. • **true**: The load balancer is enabled. • **false**: The load balancer is disabled.
http2_enable	Boolean	Specifies whether to use HTTP/2. The value can be **true** or **false**. • **true**: HTTP/2 is used. • **false**: HTTP/2 is not used. This parameter is valid only when the protocol used by the listener is set to **TERMINATED_HTTPS**.
default_pool_id	String	Specifies the ID of the associated backend server group. If a request does not match the forwarding policy, the request is forwarded to the default backend server group for processing. If the value is **null**, the listener has no default backend server group.
default_tls_container_ref	String	Specifies the ID of the server certificate used by the listener. For details, see **Certificate**. This parameter is mandatory when **protocol** is set to **TERMINATED_HTTPS**.
client_ca_tls_container_ref	String	Specifies the ID of the CA certificate used by the listener. For details, see **Certificate**.

Parameter	Type	Description
sni_container_refs	Array	Lists the IDs of SNI certificates (server certificates with domain names) used by the listener. If the parameter value is an empty list, the SNI feature is disabled.
tags	Array	Tags the listener.
created_at	String	Specifies the time when the listener was created. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format.
updated_at	String	Specifies the time when the listener was updated. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format.
tls_ciphers_policy	String	Specifies the security policy used by the listener. This parameter is valid only when the protocol used by the listener is set to **TERMINATED_HTTPS**. The value can be **tls-1-0-inherit**, **tls-1-0**, **tls-1-1**, **tls-1-2**, or **tls-1-2-strict**, and the default value is **tls-1-0**. For details of cipher suites for each security policy, see **Table 10-41**.

Table 10-55 loadbalancers parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated load balancer.

Example Request

- Example request: Querying details of a listener
  GET https://{Endpoint}/v2.0/lbaas/listeners/09e64049-2ab0-4763-a8c5-f4207875dc3e

Example Response

- Example response

```
{
    "listener": {
        "protocol_port": 8000,
        "protocol": "TCP",
        "description": "",
        "client_ca_tls_container_ref": null,
        "default_tls_container_ref": null,
        "admin_state_up": true,
        "http2_enable": false,
        "loadbalancers": [
            {
                "id": "3d77894d-2ffe-4411-ac0a-0d57689779b8"
```



```
        }
      ],
      "tenant_id": "1867112d054b427e808cc6096d8193a1",
      "project_id": "1867112d054b427e808cc6096d8193a1",
      "sni_container_refs": [],
      "connection_limit": -1,
      "default_pool_id": "b7e53dbd-62ab-4505-a280-5c066078a5c9",
      "id": "09e64049-2ab0-4763-a8c5-f4207875dc3e",
      "tags": [],
      "name": "listener-2",
      "created_at": "2018-07-25T01:54:13",
      "updated_at": "2018-07-25T01:54:14"
    }
}
```


Status Code

For details, see **Status Codes**.

10.1.2.4 Updating a Listener

Function

This API is used to update a listener, such as listener name, description, associated backend server groups, and server certificates.

Constraints

- If the provisioning status of the associated load balancer is not **ACTIVE**, the listener cannot be updated.
- Only users with the ELB administrator permissions can specify the value of **connection_limit**.
- The **default_pool_id** parameter has the following constraints:
  - Its value cannot be the ID of any backend server group of other listeners.
  - Its value cannot be the ID of any backend server group associated with the forwarding policies set for other listeners.
- The relationships between the protocol used by the listener and the protocol of the backend server group are as follows:
  - When the protocol used by the listener is **TCP**, the protocol of the backend server group must be **TCP**.
  - When the protocol used by the listener is **UDP**, the protocol of the backend server group must be **UDP**.
  - When the protocol used by the listener is **HTTP** or **TERMINATED_HTTPS**, the protocol of the backend server group must be **HTTP**.

URI

PUT /v2.0/lbaas/listeners/{listener_id}

Table 10-56 Parameter description

Parameter	Mandatory	Type	Description
listener_id	Yes	String	Specifies the listener ID.

Request

Table 10-57 Parameter description

Parameter	Mandatory	Type	Description
listener	Yes	Object	Specifies the listener. For details, see **Table 10-58**.

Table 10-58 listener parameter description

Parameter	Mandatory	Type	Description
name	No	String	Specifies the listener name. The value contains a maximum of 255 characters.
description	No	String	Provides supplementary information about the listener. The value contains a maximum of 255 characters.
connection_limit	No	Integer	Specifies the maximum number of connections. The value ranges from **-1** to **2147483647**. This parameter is reserved. Only users with the ELB administrator permissions can specify this field.
http2_enable	No	Boolean	Specifies whether to use HTTP/2. The value can be **true** or **false**. • **true**: HTTP/2 is used. • **false**: HTTP/2 is not used. This parameter is valid only when the protocol used by the listener is set to **TERMINATED_HTTPS**.

Parameter	Mandatory	Type	Description
default_pool_id	No	String	Specifies the ID of the associated backend server group. If a request does not match the forwarding policy, the request is forwarded to the default backend server group for processing. If the value is **null**, the listener has no default backend server group. This parameter has the following constraints: ● Its value cannot be the ID of any backend server group of other listeners. ● Its value cannot be the ID of any backend server group associated with the forwarding policies set for other listeners. The relationships between the protocol used by the listener and the protocol of the backend server group are as follows: ● When the protocol used by the listener is **TCP**, the protocol of the backend server group must be **TCP**. ● When the protocol used by the listener is **UDP**, the protocol of the backend server group must be **UDP**. ● When the protocol used by the listener is **HTTP** or **TERMINATED_HTTPS**, the protocol of the backend server group must be **HTTP**.
admin_state_up	No	Boolean	Specifies the administrative status of the listener. This parameter is reserved, and the default value is **true**.
default_tls_container_ref	No	String	Specifies the ID of the server certificate used by the listener. The value contains a maximum of 128 characters. **NOTE** This parameter is valid only when **protocol** is set to **TERMINATED_HTTPS**.

Parameter	Mandatory	Type	Description
client_ca_tls_container_ref	No	String	Specifies the ID of the CA certificate used by the listener. The value contains a maximum of 128 characters. **NOTE** This parameter is valid only when **protocol** is set to **TERMINATED_HTTPS**.
sni_container_refs	No	Array	Lists the IDs of SNI certificates (server certificates with domain names) used by the listener. If the parameter value is an empty list, the SNI feature is disabled. **NOTE** This parameter is valid only when **protocol** is set to **TERMINATED_HTTPS**.
tls_ciphers_policy	No	String	Specifies the security policy used by the listener. This parameter is valid only when the protocol used by the listener is set to **TERMINATED_HTTPS**. The value can be **tls-1-0-inherit**, **tls-1-0**, **tls-1-1**, **tls-1-2**, or **tls-1-2-strict**, and the default value is **tls-1-0**. For details of cipher suites for each security policy, see **Table 10-59**.

Table 10-59 tls_ciphers_policy parameter description

Security Policy	TLS Version	Cipher Suite
tls-1-0-inherit	TLS 1.2 TLS 1.1 TLS 1.0	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:DHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:AES128-SHA:AES256-SHA:DHE-DSS-AES128-SHA:CAMELLIA128-SHA:EDH-RSA-DES-CBC3-SHA:DES-CBC3-SHA:ECDHE-RSA-RC4-SHA:RC4-SHA:DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:DHE-RSA-CAMELLIA256-SHA:DHE-DSS-CAMELLIA256-SHA:CAMELLIA256-SHA:EDH-DSS-DES-CBC3-SHA:DHE-RSA-CAMELLIA128-SHA:DHE-DSS-CAMELLIA128-SHA
tls-1-0	TLS 1.2 TLS 1.1 TLS 1.0	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:AES128-SHA:AES256-SHA
tls-1-1	TLS 1.2 TLS 1.1	
tls-1-2	TLS 1.2	
tls-1-2-strict	TLS 1.2	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384

Response

Table 10-60 Response parameters

Parameter	Type	Description
listener	Object	Specifies the listener. For details, see **Table 10-61**.

Table 10-61 listeners parameter description

Parameter	Type	Description
id	String	Specifies the listener ID.
tenant_id	String	Specifies the ID of the project where the listener is used.
project_id	String	Specifies the ID of the project to which the listener belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the listener name.
description	String	Provides supplementary information about the listener.
protocol	String	Specifies the protocol used by the listener. The value can be **TCP**, **HTTP**, **UDP**, or **TERMINATED_HTTPS**.
protocol_port	Integer	Specifies the port used by the listener. The port number ranges from 1 to 65535.
loadbalancers	Array	Specifies the ID of the associated load balancer. For details, see **Table 10-44**.
connection_limit	Integer	Specifies the maximum number of connections. The value ranges from **-1** to **2147483647**. The default value is **-1**, indicating that there is no restriction on the maximum number of connections. This parameter is reserved.
admin_state_up	Boolean	Specifies the administrative status of the listener. This parameter is reserved. The value can be **true** or **false**. • **true**: The load balancer is enabled. • **false**: The load balancer is disabled.
http2_enable	Boolean	Specifies whether to use HTTP/2. The value can be **true** or **false**. • **true**: HTTP/2 is used. • **false**: HTTP/2 is not used. This parameter is valid only when the protocol used by the listener is set to **TERMINATED_HTTPS**.

Parameter	Type	Description
default_pool_id	String	Specifies the ID of the associated backend server group. If a request does not match the forwarding policy, the request is forwarded to the default backend server group for processing. If the value is **null**, the listener has no default backend server group.
default_tls_container_ref	String	Specifies the ID of the server certificate used by the listener. For details, see **Certificate**. This parameter is mandatory when **protocol** is set to **TERMINATED_HTTPS**.
client_ca_tls_container_ref	String	Specifies the ID of the CA certificate used by the listener. For details, see **Certificate**.
sni_container_refs	Array	Lists the IDs of SNI certificates (server certificates with domain names) used by the listener. If the parameter value is an empty list, the SNI feature is disabled.
tags	Array	Tags the listener.
created_at	String	Specifies the time when the listener was created. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format.
updated_at	String	Specifies the time when the listener was updated. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format.
tls_ciphers_policy	String	Specifies the security policy used by the listener. This parameter is valid only when the protocol used by the listener is set to **TERMINATED_HTTPS**. The value can be **tls-1-0-inherit**, **tls-1-0**, **tls-1-1**, **tls-1-2**, or **tls-1-2-strict**, and the default value is **tls-1-0**. For details of cipher suites for each security policy, see **Table 10-41**.

Table 10-62 loadbalancers parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated load balancer.

Example Request

- Example request: Updating a listener

```
PUT https://{Endpoint}/v2.0/lbaas/listeners/f622c150-72f5-4263-a47a-e5003c652aa3

{
   "listener": {
      "description": "my listener",
      "name": "listener-jy-test2",
      "default_pool_id": "c61310de-9a06-4f0c-850c-6f4797b9984c",
      "default_tls_container_ref": "23b58a961a4d4c95be585e98046e657a",
      "client_ca_tls_container_ref": "417a0976969f497db8cbb083bff343ba"
   }
}
```

Example Response

- Example response

```
{
   "listener": {
      "client_ca_tls_container_ref": "417a0976969f497db8cbb083bff343ba",
      "protocol": "TERMINATED_HTTPS",
      "description": "my listener",
      "default_tls_container_ref": "23b58a961a4d4c95be585e98046e657a",
      "admin_state_up": true,
      "http2_enable": false,
      "loadbalancers": [
         {
            "id": "165b6a38-5278-4569-b747-b2ee65ea84a4"
         }
      ],
      "tenant_id": "601240b9c5c94059b63d484c92cfe308",
      "project_id": "601240b9c5c94059b63d484c92cfe308",
      "sni_container_refs": [],
      "connection_limit": -1,
      "protocol_port": 443,
      "tags": [],
      "default_pool_id": "c61310de-9a06-4f0c-850c-6f4797b9984c",
      "id": "f622c150-72f5-4263-a47a-e5003c652aa3",
      "name": "listener-jy-test2",

      "created_at": "2018-07-25T01:54:13",
      "updated_at": "2018-07-25T01:54:14"

   }
}
```

Status Code

For details, see **Status Codes**.

10.1.2.5 Deleting a Listener

Function

This API is used to delete a listener by ID.

Constraints

Before deleting the listener, delete the associated backend server groups by referring to **Deleting a Backend Server Group**, or change the value of **default_pool_id** to **null** by referring to **Updating a Listener** and delete associated forwarding policies by referring to **Deleting a Forwarding Policy**.

URI

DELETE /v2.0/lbaas/listeners/{listener_id}

Table 10-63 Parameter description

Parameter	Mandatory	Type	Description
listener_id	Yes	String	Specifies the listener ID.
cascade	No	Boolean	**[Discarded]** Specifies whether to delete the resources associated with the listener when the listener is deleted, including the backend server groups and backend servers.

Request

None

Response

None

Example Request

- Example request: Deleting a listener
  DELETE https://{Endpoint}/v2.0/lbaas/listeners/35cb8516-1173-4035-8dae-0dae3453f37f

Example Response

- Example response

  None

Status Code

For details, see **Status Codes**.

10.1.3 Backend Server Group

10.1.3.1 Adding a Backend Server Group

Function

This API is used to add a backend server group. After multiple backend servers are added to a backend server group, requests are distributed among backend servers based on the load balancing algorithm configured for the backend server group and the weight set for each backend server.

Constraints

- If parameter **session-persistence** is configured, parameter **cookie_name** is available only when the value of **type** is **APP_COOKIE**.

URI

POST /v2.0/lbaas/pools

Request

Table 10-64 Parameter description

Parameter	Mandatory	Type	Description
pool	Yes	Object	Specifies the backend server group. For details, see **Table 10-65**.

Table 10-65 pool parameter description

Parameter	Mandatory	Type	Description
tenant_id	No	String	Specifies the ID of the project where the backend server group is used. The value must be the same as the value of **project_id** in the token. The value contains a maximum of 255 characters.
project_id	No	String	Specifies the ID of the project to which the backend server group belongs. This parameter has the same meaning as **tenant_id**. The value must be the same as the value of **project_id** in the token.
name	No	String	Specifies the name of the backend server group. The value contains a maximum of 255 characters.
description	No	String	Provides supplementary information about the backend server group. The value contains a maximum of 255 characters.

Parameter	Mandatory	Type	Description
protocol	Yes	String	Specifies the protocol that the backend server group uses to receive requests. TCP, UDP, and HTTP are supported. When a backend server group is associated with a listener, the relationships between the protocol used by the listener and the protocol of the backend server group are as follows: • When the protocol used by the listener is **UDP**, the protocol of the backend server group must be **UDP**. • When the protocol used by the listener is **TCP**, the protocol of the backend server group must be **TCP**. • When the protocol used by the listener is **HTTP** or **TERMINATED_HTTPS**, the protocol of the backend server group must be **HTTP**.
lb_algorithm	Yes	String	Specifies the load balancing algorithm of the backend server group. The value can be one of the following: • **ROUND_ROBIN**: indicates the weighted round robin algorithm. • **LEAST_CONNECTIONS**: indicates the weighted least connections algorithm. • **SOURCE_IP**: indicates the source IP hash algorithm. When the value is **SOURCE_IP**, the weights of backend servers in the server group are invalid.
admin_state_up	No	Boolean	Specifies the administrative status of the backend server group. This parameter is reserved, and the default value is **true**.

Parameter	Mandatory	Type	Description
listener_id	No	String	Specifies the ID of the listener associated with the backend server group. Specify either **listener_id** or **loadbalancer_id**, or both of them.
loadbalancer_id	No	String	Specifies the ID of the load balancer associated with the backend server group. Specify either **listener_id** or **loadbalancer_id**, or both of them.
session_persistence	No	Object	Specifies the sticky session timeout duration in minutes. For details, see **Table 10-66**. If the value is **null**, the sticky session feature is disabled.

Table 10-66 session_persistence parameter description

Parameter	Mandatory	Type	Description
type	Yes	String	Specifies the sticky session type. The value can be one of the following: • **SOURCE_IP**: Requests are distributed based on the client's IP address. Requests from the same IP address are sent to the same backend server. • **HTTP_COOKIE**: When the client sends a request for the first time, the load balancer automatically generates a cookie and inserts the cookie into the response message. Subsequent requests are sent to the backend server that processes the first request. • **APP_COOKIE**: When the client sends a request for the first time, the backend server that receives the request generates a cookie and inserts the cookie into the response message. Subsequent requests are sent to this backend server. When the protocol of the backend server group is TCP, only **SOURCE_IP** takes effect. When the protocol of the backend server group is HTTP, only **HTTP_COOKIE** or **APP_COOKIE** takes effect.
cookie_name	No	String	Specifies the cookie name. This parameter is mandatory when the sticky session type is **APP_COOKIE**.

Parameter	Mandatory	Type	Description
persistence_timeout	No	Integer	Specifies the sticky session timeout duration in minutes. This parameter is invalid when **type** is set to **APP_COOKIE**. The value range varies depending on the protocol of the backend server group: • When the protocol of the backend server group is TCP or UDP, the value ranges from **1** to **60**. • When the protocol of the backend server group is HTTP or HTTPS, the value ranges from **1** to **1440**.

Response

Table 10-67 Response parameters

Parameter	Type	Description
pool	Object	Specifies the backend server group. For details, see **Table 10-68**.

Table 10-68 pools parameter description

Parameter	Type	Description
id	String	Specifies the ID of the backend server group.
tenant_id	String	Specifies the ID of the project where the backend server group is used. The value contains a maximum of 255 characters.
project_id	String	Specifies the ID of the project to which the backend server group belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the name of the backend server group. The value contains a maximum of 255 characters.

Parameter	Type	Description
description	String	Provides supplementary information about the backend server group. The value contains a maximum of 255 characters.
protocol	String	Specifies the protocol that the backend server group uses to receive requests. TCP, UDP, and HTTP are supported. When a backend server group is associated with a listener, the relationships between the protocol used by the listener and the protocol of the backend server group are as follows: • When the protocol used by the listener is **UDP**, the protocol of the backend server group must be **UDP**. • When the protocol used by the listener is **TCP**, the protocol of the backend server group must be **TCP**. • When the protocol used by the listener is **HTTP** or **TERMINATED_HTTPS**, the protocol of the backend server group must be **HTTP**.
lb_algorithm	String	Specifies the load balancing algorithm of the backend server group. The value can be one of the following: • **ROUND_ROBIN**: indicates the weighted round robin algorithm. • **LEAST_CONNECTIONS**: indicates the weighted least connections algorithm. • **SOURCE_IP**: indicates the source IP hash algorithm. When the value is **SOURCE_IP**, the weights of backend servers in the server group are invalid.
members	Array	Lists the IDs of backend servers in the backend server group.
healthmonitor_id	String	Specifies the ID of the health check configured for the backend server group.
admin_state_up	Boolean	Specifies the administrative status of the backend server group. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled

Parameter	Type	Description
listeners	Array	Lists the IDs of listeners associated with the backend server group.
loadbalancers	Array	Lists the IDs of load balancers associated with the backend server group.
session_persistence	Object	Specifies whether to enable sticky sessions. For details, see **Table 10-72**. Once sticky session are enabled, requests from the same client are sent to the same backend server during the session. When sticky sessions are disabled, the value is **null**.

Table 10-69 members parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated backend server.

Table 10-70 listeners parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated backend server group.

Table 10-71 loadbalancers parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated load balancer.

Table 10-72 session_persistence parameter description

Parameter	Type	Description
type	String	Specifies the sticky session type. The value can be one of the following: • **SOURCE_IP**: Requests are distributed based on the client's IP address. Requests from the same IP address are sent to the same backend server. • **HTTP_COOKIE**: When the client sends a request for the first time, the load balancer automatically generates a cookie and inserts the cookie into the response message. Subsequent requests are sent to the backend server that processes the first request. • **APP_COOKIE**: When the client sends a request for the first time, the backend server that receives the request generates a cookie and inserts the cookie into the response message. Subsequent requests are sent to this backend server. When the protocol of the backend server group is TCP, only **SOURCE_IP** takes effect. When the protocol of the backend server group is HTTP, only **HTTP_COOKIE** or **APP_COOKIE** takes effect.
cookie_name	String	Specifies the cookie name. This parameter is mandatory when the sticky session type is **APP_COOKIE**.

Parameter	Type	Description
persistence_timeout	Integer	Specifies the sticky session timeout duration in minutes. This parameter is invalid when **type** is set to **APP_COOKIE**. • Optional value ranges are as follows: – When the protocol of the backend server group is TCP or UDP, the value ranges from **1** to **60**. – When the protocol of the backend server group is HTTP or HTTPS, the value ranges from **1** to **1440**.

Example Request

- Example request 1: Adding a backend server group with the sticky session feature disabled

```
POST https://{Endpoint}/v2.0/lbaas/pools

{
    "pool": {
        "lb_algorithm":"ROUND_ROBIN",
        "loadbalancer_id": "63ad9dfe-4750-479f-9630-ada43ccc8117",
        "protocol":"HTTP"
    }
}
```

- Example request 2: Adding an HTTP backend server group with the value of **type** set to **APP_COOKIE**

```
POST https://{Endpoint}/v2.0/lbaas/pools

{
  "pool": {
    "lb_algorithm": "ROUND_ROBIN",
    "listener_id": "370fb112-e920-486a-b051-1d0d30704dd3",
    "protocol": "HTTP",
    "session_persistence": {
      "cookie_name": "my_cookie",
      "type": "APP_COOKIE",
      "persistence_timeout": 1
    },
    "admin_state_up": true
  }
}
```

- Example request 3: Adding an HTTP backend server group with the value of **type** set to **HTTP_COOKIE**

```
POST https://{Endpoint}/v2.0/lbaas/pools

{
    "pool": {
        "lb_algorithm":"ROUND_ROBIN",
        "loadbalancer_id": "63ad9dfe-4750-479f-9630-ada43ccc8117",
        "protocol":"HTTP",
        "session_persistence":{
```



```
        "type":"HTTP_COOKIE"
      }
    }
}
```

Example Response

- Example response 1

```
{
    "pool": {
        "lb_algorithm": "ROUND_ROBIN",
        "protocol": "HTTP",
        "description": "",
        "admin_state_up": true,
        "loadbalancers": [
            {
                "id": "63ad9dfe-4750-479f-9630-ada43ccc8117"
            }
        ],
        "tenant_id": "601240b9c5c94059b63d484c92cfe308",
        "project_id": "601240b9c5c94059b63d484c92cfe308",
        "session_persistence": null,
        "healthmonitor_id": null,
        "listeners": [],
        "members": [],
        "id": "4e496951-befb-47bf-9573-c1cd11825c07",
        "name": ""
    }
}
```

- Example response 2

```
{
  "pool": {
    "lb_algorithm": "ROUND_ROBIN",
    "protocol": "HTTP",
    "description": "",
    "admin_state_up": true,
    "loadbalancers": [
      {
        "id": "6b041b9e-976b-40ba-b075-375be6110b53"
      }
    ],
    "tenant_id": "145483a5107745e9b3d80f956713e6a3",
    "project_id": "145483a5107745e9b3d80f956713e6a3",
    "session_persistence": {
      "cookie_name": "my_cookie",
      "type": "APP_COOKIE",
      "persistence_timeout": 1
    },
    "healthmonitor_id": null,
    "listeners": [
      {
        "id": "370fb112-e920-486a-b051-1d0d30704dd3"
      }
    ],
    "members": [

    ],
    "id": "307f8968-9474-4d0c-8434-66be09dabcc1",
    "name": ""
  }
}
```

- Example response 3

```
{
    "pool": {
        "lb_algorithm": "ROUND_ROBIN",
        "protocol": "HTTP",
        "description": "",
```

```
    "admin_state_up": true,
    "loadbalancers": [
        {
            "id": "63ad9dfe-4750-479f-9630-ada43ccc8117"
        }
    ],
    "tenant_id": "601240b9c5c94059b63d484c92cfe308",
    "project_id": "601240b9c5c94059b63d484c92cfe308",
    "session_persistence": {
        "persistence_timeout": 1440,
        "cookie_name": null,
        "type": "HTTP_COOKIE"
    },
    "healthmonitor_id": null,
    "listeners": [],
    "members": [],
    "id": "d46eab56-d76b-4cd3-8952-3c3c4cf113aa",
    "name": ""
  }
}
```


Status Code

For details, see **Status Codes**.

10.1.3.2 Querying Backend Server Groups

Function

This API is used to query the backend server groups and display them in a list. Filter query and pagination query are supported. Unless otherwise specified, exact match is applied.

Constraints

Parameters **marker**, **limit**, and **page_reverse** are used for pagination query. Parameters **marker** and **page_reverse** take effect only when they are used together with parameter **limit**.

URI

GET /v2.0/lbaas/pools

Request

Table 10-73 Parameter description

Parameter	Mandatory	Type	Description
marker	No	String	Specifies the ID of the backend server group from which pagination query starts, that is, the ID of the last backend server group on the previous page. If this parameter is not specified, the first page will be queried. This parameter must be used together with **limit**.
limit	No	Integer	Specifies the number of backend server groups on each page.
page_reverse	No	Boolean	Specifies the page direction. The value can be **true** or **false**, and the default value is **false**. The last page in the list requested with **page_reverse** set to **false** will not contain the "next" link, and the last page in the list requested with **page_reverse** set to **true** will not contain the "previous" link. This parameter must be used together with **limit**.
id	No	String	Specifies the ID of the backend server group.
tenant_id	No	String	Specifies the ID of the project where the backend server group is used. The value contains a maximum of 255 characters.
project_id	No	String	Specifies the ID of the project to which the backend server group belongs. This parameter has the same meaning as **tenant_id**.
name	No	String	Specifies the name of the backend server group. The value contains a maximum of 255 characters.

Parameter	Mandatory	Type	Description
description	No	String	Provides supplementary information about the backend server group. The value contains a maximum of 255 characters.
healthmonitor_id	No	String	Specifies the ID of the health check configured for the backend server group.
loadbalancer_id	No	String	Specifies the ID of the load balancer associated with the backend server group.
protocol	No	String	Specifies the protocol that the backend server group uses to receive requests. TCP, UDP, and HTTP are supported.
lb_algorithm	No	String	Specifies the load balancing algorithm of the backend server group. The value can be one of the following: • **ROUND_ROBIN**: indicates the weighted round robin algorithm. • **LEAST_CONNECTIONS**: indicates the weighted least connections algorithm. • **SOURCE_IP**: indicates the source IP hash algorithm. When the value is **SOURCE_IP**, the weights of backend servers in the server group are invalid. For details about parameter **weight**, see **Table 10-110**.
member_address	No	String	Lists the IDs of backend servers in the backend server group.
member_device_id	No	String	Specifies the ID of the cloud server used as the backend server in the backend server group.

Response

Table 10-74 Response parameters

Parameter	Type	Description
pools	Array	Specifies the backend server group. For details, see **Table 10-75**.
pools_links	List	Provides links to the previous or next page during pagination query, respectively. This parameter exists only in the response body of pagination query. For details, see **Table 10-80**.

Table 10-75 pools parameter description

Parameter	Type	Description
id	String	Specifies the ID of the backend server group.
tenant_id	String	Specifies the ID of the project where the backend server group is used. The value contains a maximum of 255 characters.
project_id	String	Specifies the ID of the project to which the backend server group belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the name of the backend server group. The value contains a maximum of 255 characters.
description	String	Provides supplementary information about the backend server group. The value contains a maximum of 255 characters.
protocol	String	Specifies the protocol that the backend server group uses to receive requests. TCP, UDP, and HTTP are supported.

Parameter	Type	Description
lb_algorithm	String	Specifies the load balancing algorithm of the backend server group. The value can be one of the following: • **ROUND_ROBIN**: indicates the weighted round robin algorithm. • **LEAST_CONNECTIONS**: indicates the weighted least connections algorithm. • **SOURCE_IP**: indicates the source IP hash algorithm. When the value is **SOURCE_IP**, the weights of backend servers in the server group are invalid.
members	Array	Lists the IDs of backend servers in the backend server group.
healthmonitor_id	String	Specifies the ID of the health check configured for the backend server group.
admin_state_up	Boolean	Specifies the administrative status of the backend server group. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
listeners	Array	Lists the IDs of listeners associated with the backend server group.
loadbalancers	String	Lists the IDs of load balancers associated with the backend server group.
session_persistence	Object	Specifies whether to enable the sticky session feature. For details, see **Table 10-79**. Once sticky session are enabled, requests from the same client are sent to the same backend server during the session. When sticky sessions are disabled, the value is **null**.

Table 10-76 members parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated backend server.

Table 10-77 listeners parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated backend server group.

Table 10-78 loadbalancers parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated load balancer.

Table 10-79 session_persistence parameter description

Parameter	Type	Description
type	String	Specifies the sticky session type. The value can be one of the following: • **SOURCE_IP**: Requests are distributed based on the client's IP address. Requests from the same IP address are sent to the same backend server. • **HTTP_COOKIE**: When the client sends a request for the first time, the load balancer automatically generates a cookie and inserts the cookie into the response message. Subsequent requests are sent to the backend server that processes the first request. • **APP_COOKIE**: When the client sends a request for the first time, the backend server that receives the request generates a cookie and inserts the cookie into the response message. Subsequent requests are sent to this backend server. When the protocol of the backend server group is TCP, only **SOURCE_IP** takes effect. When the protocol of the backend server group is HTTP, only **HTTP_COOKIE** or **APP_COOKIE** takes effect.

Parameter	Type	Description
cookie_name	String	Specifies the cookie name. This parameter is mandatory when the sticky session type is **APP_COOKIE**.
persistence_timeout	Integer	Specifies the sticky session timeout duration in minutes. This parameter is invalid when **type** is set to **APP_COOKIE**. • Optional value ranges are as follows: – When the protocol of the backend server group is TCP or UDP, the value ranges from **1** to **60**. – When the protocol of the backend server group is HTTP or HTTPS, the value ranges from **1** to **1440**.

Table 10-80 pools_links parameter description

Parameter	Type	Description
href	String	Provides links to the previous or next page during pagination query, respectively.
rel	String	Specifies the prompt of the previous or next page. The value can be **next** or **previous**. • **next**: indicates the URL of the next page. • **previous**: indicates the URL of the previous page.

Example Request

- Example request 1: Querying backend server groups by pages
  ```
  GET https://{Endpoint}/v2.0/lbaas/pools?limit=2
  ```
- Example request 2: Querying backend server groups whose load balancing algorithm is **SOURCE_IP**
  ```
  GET https://{Endpoint}/v2.0/lbaas/pools?lb_algorithm=SOURCE_IP
  ```


Example Response

- Example response 1


```
{
   "pools": [
      {
         "lb_algorithm": "SOURCE_IP",
         "protocol": "TCP",
         "description": "",
         "admin_state_up": true,
         "loadbalancers": [
            {
               "id": "07d28d4a-4899-40a3-a939-5d09d69019e1"
            }
         ],
         "tenant_id": "1867112d054b427e808cc6096d8193a1",
         "project_id": "1867112d054b427e808cc6096d8193a1",
         "session_persistence": null,
         "healthmonitor_id": null,
         "listeners": [
            {
               "id": "1b421c2d-7e78-4a78-9ee4-c8ccba41f15b"
            }
         ],
         "members": [
            {
               "id": "88f9c079-29cb-435a-b98f-0c5c0b90c2bd"
            },
            {
               "id": "2f4c9644-d5d2-4cf8-a3c0-944239a4f58c"
            }
         ],
         "id": "3a9f50bb-f041-4eac-a117-82472d8a0007",
         "name": "my-pool"
      }
   ],
   "pools_links": [
      {
      "href": "https://{Endpoint}/v2.0/lbaas/pools?
limit=2&marker=0469a5ad-6233-4669-8d38-5920f2bd95b6",
      "rel": "next"
      },
      {
      "href": "https://{Endpoint}/v2.0/lbaas/pools?limit=2&marker=02d43e35-e874-4139-bdba-
d65609db20ab&page_reverse=True",
      "rel": "previous"
      }
   ]
}
```


- Example response 2


```
{
   "pools": [
      {
         "lb_algorithm": "SOURCE_IP",
         "protocol": "TCP",
         "description": "",
         "admin_state_up": true,
         "loadbalancers": [
            {
               "id": "07d28d4a-4899-40a3-a939-5d09d69019e1"
            }
         ],
         "tenant_id": "1867112d054b427e808cc6096d8193a1",
         "project_id": "1867112d054b427e808cc6096d8193a1",
         "session_persistence": null,
         "healthmonitor_id": null,
         "listeners": [
            {
               "id": "1b421c2d-7e78-4a78-9ee4-c8ccba41f15b"
```



```
            }
        ],
        "members": [
            {
                "id": "88f9c079-29cb-435a-b98f-0c5c0b90c2bd"
            },
            {
                "id": "2f4c9644-d5d2-4cf8-a3c0-944239a4f58c"
            }
        ],
        "id": "3a9f50bb-f041-4eac-a117-82472d8a0007",
        "name": "my-pool"
    }
  ]
}
```


Status Code

For details, see **Status Codes**.

10.1.3.3 Querying Details of a Backend Server Group

Function

This API is used to query details about a backend server group using its ID.

URI

GET /v2.0/lbaas/pools/{pool_id}

Table 10-81 Parameter description

Parameter	Mandatory	Type	Description
pool_id	Yes	String	Specifies the ID of the backend server group.

Request

None

Response

Table 10-82 Response parameters

Parameter	Type	Description
pool	Object	Specifies the backend server group. For details, see **Table 10-83**.

Table 10-83 pools parameter description

Parameter	Type	Description
id	String	Specifies the ID of the backend server group.
tenant_id	String	Specifies the ID of the project where the backend server group is used. The value contains a maximum of 255 characters.
project_id	String	Specifies the ID of the project to which the backend server group belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the name of the backend server group. The value contains a maximum of 255 characters.
description	String	Provides supplementary information about the backend server group. The value contains a maximum of 255 characters.
protocol	String	Specifies the protocol that the backend server group uses to receive requests. TCP, UDP, and HTTP are supported. When a backend server group is associated with a listener, the relationships between the protocol used by the listener and the protocol of the backend server group are as follows: • When the protocol used by the listener is **UDP**, the protocol of the backend server group must be **UDP**. • When the protocol used by the listener is **TCP**, the protocol of the backend server group must be **TCP**. • When the protocol used by the listener is **HTTP** or **TERMINATED_HTTPS**, the protocol of the backend server group must be **HTTP**.

Parameter	Type	Description
lb_algorithm	String	Specifies the load balancing algorithm of the backend server group. The value can be one of the following: • **ROUND_ROBIN**: indicates the weighted round robin algorithm. • **LEAST_CONNECTIONS**: indicates the weighted least connections algorithm. • **SOURCE_IP**: indicates the source IP hash algorithm. When the value is **SOURCE_IP**, the weights of backend servers in the server group are invalid.
members	Array	Lists the IDs of backend servers in the backend server group.
healthmonitor_id	String	Specifies the ID of the health check configured for the backend server group.
admin_state_up	Boolean	Specifies the administrative status of the backend server group. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
listeners	Array	Lists the IDs of listeners associated with the backend server group.
loadbalancers	Array	Lists the IDs of load balancers associated with the backend server group.
session_persistence	Object	Specifies whether to enable sticky sessions. For details, see **Table 10-72**. Once sticky session are enabled, requests from the same client are sent to the same backend server during the session. When sticky sessions are disabled, the value is **null**.

Table 10-84 members parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated backend server.

Table 10-85 listeners parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated backend server group.

Table 10-86 loadbalancers parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated load balancer.

Table 10-87 session_persistence parameter description

Parameter	Type	Description
type	String	Specifies the sticky session type. The value can be one of the following: • **SOURCE_IP**: Requests are distributed based on the client's IP address. Requests from the same IP address are sent to the same backend server. • **HTTP_COOKIE**: When the client sends a request for the first time, the load balancer automatically generates a cookie and inserts the cookie into the response message. Subsequent requests are sent to the backend server that processes the first request. • **APP_COOKIE**: When the client sends a request for the first time, the backend server that receives the request generates a cookie and inserts the cookie into the response message. Subsequent requests are sent to this backend server. When the protocol of the backend server group is TCP, only **SOURCE_IP** takes effect. When the protocol of the backend server group is HTTP, only **HTTP_COOKIE** or **APP_COOKIE** takes effect.

Parameter	Type	Description
cookie_name	String	Specifies the cookie name. This parameter is mandatory when the sticky session type is **APP_COOKIE**.
persistence_timeout	Integer	Specifies the sticky session timeout duration in minutes. This parameter is invalid when **type** is set to **APP_COOKIE**. • Optional value ranges are as follows: – When the protocol of the backend server group is TCP or UDP, the value ranges from **1** to **60**. – When the protocol of the backend server group is HTTP or HTTPS, the value ranges from **1** to **1440**.

Example Request

- Example request: Querying details of a backend server group
  ```
  GET https://{Endpoint}/v2.0/lbaas/pools/5a9a3e9e-d1aa-448e-af37-a70171f2a332
  ```

Example Response

- Example response
  ```
  {
      "pool": {
          "lb_algorithm": "SOURCE_IP",
          "protocol": "TCP",
          "description": "",
          "admin_state_up": true,
          "loadbalancers": [
              {
                  "id": "6f52004c-3fe9-4c09-b8ce-ed9d9c74a3b1"
              }
          ],
          "tenant_id": "1867112d054b427e808cc6096d8193a1",
          "project_id": "1867112d054b427e808cc6096d8193a1",
          "session_persistence": null,
          "healthmonitor_id": null,
          "listeners": [
              {
                  "id": "6e29b2cd-4e53-40f6-ae7b-29e918de67f2"
              }
          ],
          "members": [],
          "id": "5a9a3e9e-d1aa-448e-af37-a70171f2a332",
          "name": "my-pool"
      }
  }
  ```


Status Code

For details, see **Status Codes**.

10.1.3.4 Updating a Backend Server Group

Function

This API is used to update a backend server group.

Constraints

If the provisioning status of the load balancer associated with a backend server group is not **ACTIVE**, the backend server group cannot be updated.

URI

PUT /v2.0/lbaas/pools/{pool_id}

Table 10-88 Parameter description

Parameter	Mandatory	Type	Description
pool_id	Yes	String	Specifies the ID of the backend server group.

Request

Table 10-89 Parameter description

Parameter	Mandatory	Type	Description
pool	Yes	Object	Specifies the backend server group. For details, see **Table 10-90**.

Table 10-90 pool parameter description

Parameter	Mandatory	Type	Description
name	No	String	Specifies the name of the backend server group. The value contains a maximum of 255 characters.

Parameter	Mandatory	Type	Description
description	No	String	Provides supplementary information about the backend server group. The value contains a maximum of 255 characters.
lb_algorithm	No	String	Specifies the load balancing algorithm of the backend server group. Value options: • **ROUND_ROBIN**: indicates the weighted round robin algorithm. • **LEAST_CONNECTIONS**: indicates the weighted least connections algorithm. • **SOURCE_IP**: indicates the source IP hash algorithm. When the value is **SOURCE_IP**, the weights of backend servers in the server group are invalid.
admin_state_up	No	Boolean	Specifies the administrative status of the backend server group. This parameter is reserved, and the default value is **true**.
session_persistence	No	Object	Specifies whether to enable the sticky session feature. For details, see **Table 10-97**. Once sticky session are enabled, requests from the same client are sent to the same backend server during the session. When sticky sessions are disabled, the value is **null**.

Table 10-91 session_persistence parameter description

Parameter	Mandatory	Type	Description
type	No	String	Specifies the sticky session type. Value options: • **SOURCE_IP**: Requests are distributed based on the client's IP address. Requests from the same IP address are sent to the same backend server. • **HTTP_COOKIE**: When the client sends a request for the first time, the load balancer automatically generates a cookie and inserts the cookie into the response message. Subsequent requests are sent to the backend server that processes the first request. • **APP_COOKIE**: When the client sends a request for the first time, the backend server that receives the request generates a cookie and inserts the cookie into the response message. Subsequent requests are sent to this backend server. • When the protocol of the backend server group is TCP, only **SOURCE_IP** takes effect. When the protocol of the backend server group is HTTP, only **HTTP_COOKIE** or **APP_COOKIE** takes effect.
cookie_name	No	String	Specifies the cookie name. This parameter is mandatory and can be specified when the sticky session type is **APP_COOKIE**.
persistence_timeout	No	Integer	Specifies the sticky session timeout duration in minutes. This parameter is invalid when **type** is set to **APP_COOKIE**. Value range options are as follows: • When the protocol of the backend server group is TCP or UDP, the value ranges from **1** to **60**. • When the protocol of the backend server group is HTTP or HTTPS, the value ranges from **1** to **1440**.

Response

Table 10-92 Parameter description

Parameter	Type	Description
pool	Object	Specifies the backend server group. For details, see **Table 10-93**.

Table 10-93 pools parameter description

Parameter	Type	Description
id	String	Specifies the ID of the backend server group.
tenant_id	String	Specifies the ID of the project where the backend server group is used. The value contains a maximum of 255 characters.
project_id	String	Specifies the ID of the project to which the backend server group belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the name of the backend server group. The value contains a maximum of 255 characters.
description	String	Provides supplementary information about the backend server group. The value contains a maximum of 255 characters.

Parameter	Type	Description
protocol	String	Specifies the protocol that the backend server group uses to receive requests. TCP, UDP, and HTTP are supported. When a backend server group is associated with a listener, the relationships between the protocol used by the listener and the protocol of the backend server group are as follows: • When the protocol used by the listener is **UDP**, the protocol of the backend server group must be **UDP**. • When the protocol used by the listener is **TCP**, the protocol of the backend server group must be **TCP**. • When the protocol used by the listener is **HTTP** or **TERMINATED_HTTPS**, the protocol of the backend server group must be **HTTP**.
lb_algorithm	String	Specifies the load balancing algorithm of the backend server group. The value can be one of the following: • **ROUND_ROBIN**: indicates the weighted round robin algorithm. • **LEAST_CONNECTIONS**: indicates the weighted least connections algorithm. • **SOURCE_IP**: indicates the source IP hash algorithm. When the value is **SOURCE_IP**, the weights of backend servers in the server group are invalid.
members	Array	Lists the IDs of backend servers in the backend server group.
healthmonitor_id	String	Specifies the ID of the health check configured for the backend server group.
admin_state_up	Boolean	Specifies the administrative status of the backend server group. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
listeners	Array	Lists the IDs of listeners associated with the backend server group.

Parameter	Type	Description
loadbalancers	Array	Lists the IDs of load balancers associated with the backend server group.
session_persistence	Object	Specifies whether to enable sticky sessions. For details, see **Table 10-72**. Once sticky session are enabled, requests from the same client are sent to the same backend server during the session. When sticky sessions are disabled, the value is **null**.

Table 10-94 members parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated backend server.

Table 10-95 listeners parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated backend server group.

Table 10-96 loadbalancers parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated load balancer.

Table 10-97 session_persistence parameter description

Parameter	Type	Description
type	String	Specifies the sticky session type. The value can be one of the following: • **SOURCE_IP**: Requests are distributed based on the client's IP address. Requests from the same IP address are sent to the same backend server. • **HTTP_COOKIE**: When the client sends a request for the first time, the load balancer automatically generates a cookie and inserts the cookie into the response message. Subsequent requests are sent to the backend server that processes the first request. • **APP_COOKIE**: When the client sends a request for the first time, the backend server that receives the request generates a cookie and inserts the cookie into the response message. Subsequent requests are sent to this backend server. When the protocol of the backend server group is TCP, only **SOURCE_IP** takes effect. When the protocol of the backend server group is HTTP, only **HTTP_COOKIE** or **APP_COOKIE** takes effect.
cookie_name	String	Specifies the cookie name. This parameter is mandatory when the sticky session type is **APP_COOKIE**.

Parameter	Type	Description
persistence_timeout	Integer	Specifies the sticky session timeout duration in minutes. This parameter is invalid when **type** is set to **APP_COOKIE**. • Optional value ranges are as follows: – When the protocol of the backend server group is TCP or UDP, the value ranges from **1** to **60**. – When the protocol of the backend server group is HTTP or HTTPS, the value ranges from **1** to **1440**.

Example Request

- Example request 1: Updating a backend server group

```
PUT https://{Endpoint}/v2.0/lbaas/pools/12ff63af-4127-4074-a251-bcb2ecc53ebe

{
    "pool": {
        "name": "pool2",
        "description": "pool two",
        "lb_algorithm": "LEAST_CONNECTIONS"
    }
}
```

- Example request 2: Disabling the sticky session feature of a backend server group

```
PUT https://{Endpoint}/v2.0/lbaas/pools/d46eab56-d76b-4cd3-8952-3c3c4cf113aa

{
    "pool": {
        "session_persistence":null
    }
}
```

Example Response

- Example response 1

```
{
    "pool": {
        "lb_algorithm": "LEAST_CONNECTIONS",
        "protocol": "HTTP",
        "description": "pool two",
        "loadbalancers": [
            {
                "id": "63ad9dfe-4750-479f-9630-ada43ccc8117"
            }
        ],
        "admin_state_up": true,
        "tenant_id": "1a3e005cf9ce40308c900bcb08e5320c",
        "project_id": "1a3e005cf9ce40308c900bcb08e5320c",
        "session_persistence": {
            "cookie_name": null,
            "type": "HTTP_COOKIE",
```



```
            "persistence_timeout": 1
        },
        "healthmonitor_id": null,
        "listeners": [
            {
                "id": "39de4d56-d663-46e5-85a1-5b9d5fa17829"
            }
        ],
        "members": [],
        "id": "12ff63af-4127-4074-a251-bcb2ecc53ebe",
        "name": "pool2"
    }
}
```


- Example response 2


```
{
    "pool": {
        "lb_algorithm": "ROUND_ROBIN",
        "protocol": "HTTP",
        "description": "",
        "admin_state_up": true,
        "loadbalancers": [
            {
                "id": "63ad9dfe-4750-479f-9630-ada43ccc8117"
            }
        ],
        "tenant_id": "601240b9c5c94059b63d484c92cfe308",
        "project_id": "601240b9c5c94059b63d484c92cfe308",
        "session_persistence": null,
        "healthmonitor_id": null,
        "listeners": [],
        "members": [],
        "id": "d46eab56-d76b-4cd3-8952-3c3c4cf113aa",
        "name": ""
    }
}
```


Status Code

For details, see **Status Codes**.

10.1.3.5 Deleting a Backend Server Group

Function

This API is used to delete a backend server group.

Constraints

Before deleting a backend server group, remove all backend servers, delete the health check, and disassociate forwarding policies from the backend server group by changing the value of **redirect_pool_id** to **null**. For details, see **Updating a Forwarding Policy**.

URI

DELETE /v2.0/lbaas/pools/{pool_id}

Table 10-98 Parameter description

Parameter	Mandatory	Type	Description
pool_id	Yes	String	Specifies the ID of the backend server group.

Request

None

Response

None

Example Request

- Example request: Deleting a backend server group
  ```
  DELETE /v2.0/lbaas/pools/5a9a3e9e-d1aa-448e-af37-a70171f2a332
  ```

Example Response

- Example response

  None

Status Code

For details, see **Status Codes**.

10.1.4 Backend Server

10.1.4.1 Adding a Backend Server

Function

This API is used to add a backend server to a specific backend server group. After a backend server group is added to a listener, traffic is distributed to backend servers in this server group using the specified load balancing algorithm.

Constraints

Two backend servers in a backend server group cannot have the same private IP address or port number.

The subnet specified during server creation must be in the same VPC as the subnet from which the private IP address of the load balancer is assigned.

URI

POST /v2.0/lbaas/pools/{pool_id}/members

Table 10-99 Parameter description

Parameter	Mandatory	Type	Description
pool_id	Yes	String	Specifies the ID of the backend server group.

Request

Table 10-100 Parameter description

Parameter	Mandatory	Type	Description
member	Yes	Object	Specifies the backend server. For details, see **Table 10-101**.

Table 10-101 member parameter description

Parameter	Mandatory	Type	Description
tenant_id	No	String	Specifies the ID of the project where the backend server is used. The value must be the same as the value of **project_id** in the token. The value contains a maximum of 255 characters.
project_id	No	String	Specifies the ID of the project to which the backend server belongs. This parameter has the same meaning as **tenant_id**. The value must be the same as the value of **project_id** in the token.
name	No	String	Specifies the backend server name. The value is an empty character string by default. The value contains a maximum of 255 characters.

Parameter	Mandatory	Type	Description
address	Yes	String	Specifies the private IP address of the backend server. This IP address must be in the subnet specified by **subnet_id**. This parameter can be set only to the IP address of the primary NIC, for example, 192.168.3.11. The value contains a maximum of 64 characters.
protocol_port	Yes	Integer	Specifies the port used by the backend server. The port number ranges from 1 to 65535.
subnet_id	Yes	String	Specifies the ID of the subnet where the backend server works. The private IP address of the backend server is in this subnet. Only IPv4 subnets are supported.
admin_state_up	No	Boolean	Specifies the administrative status of the backend server. This parameter is reserved, and the default value is **true**.
weight	No	Integer	Specifies the backend server weight. The value ranges from **0** to **100**. If the value is **0**, the backend server will not accept new requests. The default value is **1**.

Response

Table 10-102 Response parameters

Parameter	Type	Description
member	Object	Specifies the backend server. For details, see **Table 10-103**.

Table 10-103 member parameter description

Parameter	Type	Description
id	String	Specifies the backend server ID. **NOTE** The value of this parameter is not the ID of server. It is the ID automatically generated for the backend server associated with the load balancer.
tenant_id	String	Specifies the ID of the project where the backend server is used. The value contains a maximum of 255 characters.
project_id	String	Specifies the ID of the project to which the backend server belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the backend server name. The value contains a maximum of 255 characters.
address	String	Specifies the private IP address of the backend server. This IP address must be in the subnet specified by **subnet_id**. This parameter can be set only to the IP address of the primary NIC, for example, 192.168.3.11. The value contains a maximum of 64 characters.
protocol_port	Integer	Specifies the port used by the backend server. The port number ranges from 1 to 65535.
subnet_id	String	Specifies the ID of the subnet where the backend server works. The private IP address of the backend server is in this subnet. IPv6 subnets are not supported.
admin_state_up	Boolean	Specifies the administrative status of the backend server. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled

Parameter	Type	Description
weight	Integer	Specifies the backend server weight. The value ranges from **0** to **100**. If the value is **0**, the backend server will not accept new requests. The default value is **1**.
operating_status	String	Specifies the health check result of the backend server. The value can be one of the following: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group that the backend server belongs to. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist.

Example Request

- Step 1: Query the subnet ID and IP address using the server ID. **device_id** in the request indicates the server ID. Obtain the values of **subnet_id** and **ip_address** of the primary NIC (the port for which **primary_interface** is **true**) in the response body.

  ```
  GET https://{VPCEndpoint}/v2.0/ports?device_id=f738c464-b5c2-45df-86c0-7f436620cd54
  ```

  Example response

  ```
  {
     "ports": [
        {
           "id": "94971c39-46f0-443a-85e8-31cb7497c78e",
           "name": "",
           "status": "ACTIVE",
           "admin_state_up": true,
           "fixed_ips": [
              {
                 "subnet_id": "33d8b01a-bbe6-41f4-bc45-78a1d284d503",
                 "ip_address": "192.168.44.11"
              }
           ],
           "mac_address": "fa:16:3e:5c:d2:57",
           "network_id": "1b76b9c2-9b7e-4ced-81bd-d13f7389d7c9",
           "tenant_id": "04dd36f978800fe22f9bc00bea090736",
           "project_id": "04dd36f978800fe22f9bc00bea090736",
           "device_id": "f738c464-b5c2-45df-86c0-7f436620cd54",
           "device_owner": "compute:xx-xxxx-4a",
           "security_groups": [
              "a10dfc31-0055-4b84-b36e-1291b918125c",
              "7a233393-5be2-4dff-8360-1558dd950f6e"
           ],
           "extra_dhcp_opts": [],
           "allowed_address_pairs": [],
           "binding:vnic_type": "normal",
           "binding:vif_details": {
              "primary_interface": true
  ```



```
            },
            "binding:profile": {},
            "port_security_enabled": true,
            "created_at": "2019-11-12T17:17:51",
            "updated_at": "2019-11-12T17:17:51"
        }
    ]
}
```

- Step 2: Use the subnet ID and IP address obtained in **▪ Step 1** to add a backend server.

```
POST https://{Endpoint}/v2.0/lbaas/pools/5a9a3e9e-d1aa-448e-af37-a70171f2a332/members

{
    "member": {
        "subnet_id": "33d8b01a-bbe6-41f4-bc45-78a1d284d503",
        "protocol_port": 88,
        "name": "member-jy-tt-1",
        "address": "192.168.44.11"
    }
}
```

Example Response

- Example response

```
{
    "member": {
        "name": "member-jy-tt-1",
        "weight": 1,
        "admin_state_up": true,
        "subnet_id": "33d8b01a-bbe6-41f4-bc45-78a1d284d503",
        "tenant_id": "145483a5107745e9b3d80f956713e6a3",
        "project_id": "145483a5107745e9b3d80f956713e6a3",
        "address": "192.168.44.11",
        "protocol_port": 88,
        "operating_status": "ONLINE",
        "id": "c0042496-e220-44f6-914b-e6ca33bab503"
    }
}
```

Status Code

For details, see **Status Codes**.

10.1.4.2 Querying Backend Servers

Function

This API is used to query backend servers in a specific backend server group. Filter query and pagination query are supported. Unless otherwise specified, exact match is applied.

Constraints

Parameters **marker**, **limit**, and **page_reverse** are used for pagination query. Parameters **marker** and **page_reverse** take effect only when they are used together with parameter **limit**.

URI

GET /v2.0/lbaas/pools/{pool_id}/members

Table 10-104 Parameter description

Parameter	Mandatory	Type	Description
pool_id	Yes	String	Specifies the ID of the backend server group.

Request

Table 10-105 Parameter description

Parameter	Mandatory	Type	Description
marker	No	String	Specifies the ID of the backend server from which pagination query starts, that is, the ID of the last backend server on the previous page. If this parameter is not specified, the first page will be queried. This parameter must be used together with **limit**.
limit	No	Integer	Specifies the number of backend servers on each page. If this parameter is not set, all backend servers are queried by default.
page_reverse	No	Boolean	Specifies the page direction. The value can be **true** or **false**, and the default value is **false**. The last page in the list requested with **page_reverse** set to **false** will not contain the "next" link, and the last page in the list requested with **page_reverse** set to **true** will not contain the "previous" link. This parameter must be used together with **limit**.
id	No	String	Specifies the backend server ID. **NOTE** The value of this parameter is not the ID of server. It is the ID automatically generated for the backend server associated with the load balancer.

Parameter	Mandatory	Type	Description
tenant_id	No	String	Specifies the ID of the project where the backend server is used. The value contains a maximum of 255 characters.
project_id	No	String	Specifies the ID of the project to which the backend server belongs. This parameter has the same meaning as **tenant_id**.
name	No	String	Specifies the backend server name. The value contains a maximum of 255 characters. **NOTE** The value of this parameter is not the name of server. It is the name automatically generated for the backend server associated with the load balancer.
address	No	String	Specifies the private IP address of the backend server. The value contains a maximum of 64 characters.
protocol_port	No	Integer	Specifies the port used by the backend server.
subnet_id	No	String	Specifies the ID of the subnet where the backend server works.
admin_state_up	No	Boolean	Specifies the administrative status of the backend server. This parameter is reserved, and the default value is **true**.
weight	No	Integer	Specifies the backend server weight.

Response

Table 10-106 Response parameters

Parameter	Type	Description
members	Array	Lists the backend servers in the backend server group. For details, see **Table 10-107**.

Parameter	Type	Description
members_links	Array	Provides links to the previous or next page during pagination query, respectively. This parameter exists only in the response body of pagination query. For details, see **Table 10-108**.

Table 10-107 members parameter description

Parameter	Type	Description
id	String	Specifies the backend server ID. **NOTE** The value of this parameter is not the ID of server. It is the ID automatically generated for the backend server associated with the load balancer.
tenant_id	String	Specifies the ID of the project where the backend server is used. The value contains a maximum of 255 characters.
project_id	String	Specifies the ID of the project to which the backend server belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the backend server name. The value contains a maximum of 255 characters.
address	String	Specifies the private IP address of the backend server. This IP address must be in the subnet specified by **subnet_id**. This parameter can be set only to the IP address of the primary NIC, for example, 192.168.3.11. The value contains a maximum of 64 characters.
protocol_port	Integer	Specifies the port used by the backend server. The port number ranges from 1 to 65535.
subnet_id	String	Specifies the ID of the subnet where the backend server works. The private IP address of the backend server is in this subnet. IPv6 subnets are not supported.

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the backend server. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
weight	Integer	Specifies the backend server weight. The value ranges from **0** to **100**. If the value is **0**, the backend server will not accept new requests. The default value is **1**.
operating_status	String	Specifies the operating status of the load balancer. This parameter is reserved, and its value can be **ONLINE** or **FROZEN**.

Table 10-108 members_links parameter description

Parameter	Type	Description
href	String	Provides links to the previous or next page during pagination query, respectively.
rel	String	Specifies the prompt of the previous or next page. The value can be **next** or **previous**. • **next**: indicates the URL of the next page. • **previous**: indicates the URL of the previous page.

Example Request

- Example request 1: Querying all backend servers
  ```
  GET https://{Endpoint}/v2.0/lbaas/pools/5a9a3e9e-d1aa-448e-af37-a70171f2a332/members
  ```
- Example request 2: Querying the backend cloud server whose IP address is 10.0.0.8 and port number is 80
  ```
  GET https://{Endpoint}/v2.0/lbaas/pools/5a9a3e9e-d1aa-448e-af37-a70171f2a332/members?address=10.0.0.8&protocol_port=80
  ```

Example Response

- Example response 1
  ```
  {
    "members": [
      {
        "address": "10.0.0.8",
        "admin_state_up": true,
  ```



```
            "id": "9a7aff27-fd41-4ec1-ba4c-3eb92c629313",
            "protocol_port": 80,
            "subnet_id": "013d3059-87a4-45a5-91e9-d721068ae0b2",
            "tenant_id": "1a3e005cf9ce40308c900bcb08e5320c",
            "project_id": "1a3e005cf9ce40308c900bcb08e5320c",
            "weight": 1,
            "operating_status": "ONLINE",
            "name": "member-name"
        }
    ]
}
```


- Example response 2


```
{
    "members": [
        {
            "address": "10.0.0.8",
            "admin_state_up": true,
            "id": "9a7aff27-fd41-4ec1-ba4c-3eb92c629313",
            "protocol_port": 80,
            "subnet_id": "013d3059-87a4-45a5-91e9-d721068ae0b2",
            "tenant_id": "1a3e005cf9ce40308c900bcb08e5320c",
            "project_id": "1a3e005cf9ce40308c900bcb08e5320c",
            "weight": 1,
            "operating_status": "ONLINE",
            "name": "member-name"
        }
    ]
}
```


Status Code

For details, see **Status Codes**.

10.1.4.3 Querying Details of a Backend Server

Function

This API is used to query details about a backend server.

URI

GET /v2.0/lbaas/pools/{pool_id}/members/{member_id}

Table 10-109 Parameter description

Parameter	Mandatory	Type	Description
pool_id	Yes	String	Specifies the ID of the backend server group.

Parameter	Mandatory	Type	Description
member_id	Yes	String	Specifies the backend server ID. **NOTE** • The value of this parameter is not the ID of server. It is the ID automatically generated for the backend server associated with the load balancer. • You can obtain this value by calling the API described in **Querying Backend Servers**.

Request

None

Response

Table 10-110 Response parameters

Parameter	Type	Description
member	Object	Lists the backend servers. For details, see **Table 10-111**.

Table 10-111 member parameter description

Parameter	Type	Description
id	String	Specifies the backend server ID. **NOTE** The value of this parameter is not the ID of server. It is the ID automatically generated for the backend server associated with the load balancer.
tenant_id	String	Specifies the ID of the project where the backend server is used. The value contains a maximum of 255 characters.
project_id	String	Specifies the ID of the project to which the backend server belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the backend server name. The value contains a maximum of 255 characters.

Parameter	Type	Description
address	String	Specifies the private IP address of the backend server. This IP address must be in the subnet specified by **subnet_id**. This parameter can be set only to the IP address of the primary NIC, for example, 192.168.3.11. The value contains a maximum of 64 characters.
protocol_port	Integer	Specifies the port used by the backend server. The port number ranges from 1 to 65535.
subnet_id	String	Specifies the ID of the subnet where the backend server works. The private IP address of the backend server is in this subnet. IPv6 subnets are not supported.
admin_state_up	Boolean	Specifies the administrative status of the backend server. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
weight	Integer	Specifies the backend server weight. The value ranges from **0** to **100**. If the value is **0**, the backend server will not accept new requests. The default value is **1**.
operating_status	String	Specifies the health check result of the backend server. The value can be one of the following: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group that the backend server belongs to. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist.

Example Request

- Example request: Querying details of a backend server
  ```
  GET https://{Endpoint}/v2.0/lbaas/pools/5a9a3e9e-d1aa-448e-af37-a70171f2a332/members/cf024846-7516-4e3a-b0fb-6590322c836f
  ```

Example Response

- Example response
  ```
  {
     "member": {
        "name": "",
        "weight": 1,
        "admin_state_up": true,
        "subnet_id": "823d5866-6e30-45c2-9b1a-a1ebc3757fdb",
        "tenant_id": "145483a5107745e9b3d80f956713e6a3",
        "project_id": "145483a5107745e9b3d80f956713e6a3",
        "address": "192.172.3.100",
        "protocol_port": 8080,
        "operating_status": "ONLINE",
        "id": "e58f5bfa-0e46-4bc5-951c-8473d3e5f24a"
     }
  }
  ```

Status Code

For details, see **Status Codes**.

10.1.4.4 Updating a Backend Server

Function

This API is used to update a backend server. You can modify its name and weight. You can set a larger weight for backend servers that can receive more traffic.

Constraints

If the provisioning status of the associated load balancer is not **ACTIVE**, the backend server cannot be updated.

URI

PUT /v2.0/lbaas/pools/{pool_id}/members/{member_id}

Table 10-112 Parameter description

Parameter	Mandatory	Type	Description
pool_id	Yes	String	Specifies the ID of the backend server group.

Parameter	Mandatory	Type	Description
member_id	Yes	String	Specifies the backend server ID. **NOTE** • The value of this parameter is not the ID of server. It is the ID automatically generated for the backend server associated with the load balancer. • You can obtain this value by calling the API described in **Querying Backend Servers**.

Request

Table 10-113 Parameter description

Parameter	Mandatory	Type	Description
member	Yes	Object	Specifies the backend server. For details, see **Table 10-114**.

Table 10-114 member parameter description

Parameter	Mandatory	Type	Description
name	No	String	Specifies the backend server name. The value contains a maximum of 255 characters.
admin_state_up	No	Boolean	Specifies the administrative status of the backend server. This parameter is reserved, and the default value is **true**.
weight	No	Integer	Specifies the backend server weight. The value ranges from **0** to **100**. If the value is **0**, the backend server will not accept new requests. The default value is **1**.

Response

Table 10-115 Response parameters

Parameter	Type	Description
member	Object	Specifies the backend server. For details, see **Table 10-116**.

Table 10-116 member parameter description

Parameter	Type	Description
id	String	Specifies the backend server ID. **NOTE** The value of this parameter is not the ID of server. It is the ID automatically generated for the backend server associated with the load balancer.
tenant_id	String	Specifies the ID of the project where the backend server is used. The value contains a maximum of 255 characters.
project_id	String	Specifies the ID of the project to which the backend server belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the backend server name. The value contains a maximum of 255 characters.
address	String	Specifies the private IP address of the backend server. This IP address must be in the subnet specified by **subnet_id**. This parameter can be set only to the IP address of the primary NIC, for example, 192.168.3.11. The value contains a maximum of 64 characters.
protocol_port	Integer	Specifies the port used by the backend server. The port number ranges from 1 to 65535.
subnet_id	String	Specifies the ID of the subnet where the backend server works. The private IP address of the backend server is in this subnet. IPv6 subnets are not supported.

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the backend server. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
weight	Integer	Specifies the backend server weight. The value ranges from **0** to **100**. If the value is **0**, the backend server will not accept new requests. The default value is **1**.
operating_status	String	Specifies the health check result of the backend server. The value can be one of the following: • **ONLINE**: The backend server is running normally. • **NO_MONITOR**: No health check is configured for the backend server group that the backend server belongs to. • **OFFLINE**: The cloud server used as the backend server is stopped or does not exist.

Example Request

- Example request: Updating the name and weight of a backend server

```
PUT https://{Endpoint}/v2.0/lbaas/pools/5a9a3e9e-d1aa-448e-af37-a70171f2a332/members/c0042496-e220-44f6-914b-e6ca33bab503

{
    "member": {
        "name": "member create test",
        "weight": 10
    }
}
```

Example Response

- Example response

```
{
    "member": {
        "name": "member-jy-tt-1",
        "weight": 1,
        "admin_state_up": true,
        "subnet_id": "33d8b01a-bbe6-41f4-bc45-78a1d284d503",
        "tenant_id": "145483a5107745e9b3d80f956713e6a3",
        "project_id": "145483a5107745e9b3d80f956713e6a3",
        "address": "192.168.44.11",
        "protocol_port": 88,
        "operating_status": "ONLINE",
```



```
    "id": "c0042496-e220-44f6-914b-e6ca33bab503"
  }
}
```

Status Code

For details, see **Status Codes**.

10.1.4.5 Removing a Backend Server

Function

This API is used to remove a backend server by its ID.

Constraints

After you remove a backend server, new connections to this server will not be established. However, long connections that have been established will be maintained.

URI

DELETE /v2.0/lbaas/pools/{pool_id}/members/{member_id}

Table 10-117 Parameter description

Parameter	Mandatory	Type	Description
pool_id	Yes	String	Specifies the ID of the backend server group.
member_id	Yes	String	Specifies the backend server ID. **NOTE** • The value of this parameter is not the ID of server. It is the ID automatically generated for the backend server associated with the load balancer. • You can obtain this value by calling the API described in **Querying Backend Servers**.

Request

None

Response

None

Example Request

- Example request: Removing a backend server
  ```
  DELETE https://{Endpoint}/v2.0/lbaas/pools/5a9a3e9e-d1aa-448e-af37-a70171f2a332/members/cf024846-7516-4e3a-b0fb-6590322c836f
  ```

Example Response

- Example response

  None

Status Code

For details, see **Status Codes**.

10.1.5 Health Check

10.1.5.1 Configuring a Health Check

Function

This API is used to configure a health check for a backend server group to check the status of backend servers. If the health check result is **OFFLINE**, backend servers are considered unhealthy. You need to check the server configuration.

Constraints

The security group must allow access from 100.125.0.0/16. Otherwise, the health check cannot be performed.

If UDP is used for the health check, the protocol of the backend server group must be UDP.

URI

POST /v2.0/lbaas/healthmonitors

Request

Table 10-118 Parameter description

Parameter	Mandatory	Type	Description
healthmonitor	Yes	Object	Specifies the health check. For details, see **Table 10-119**.

Table 10-119 healthmonitor parameter description

Parameter	Mandatory	Type	Description
tenant_id	No	String	Specifies the ID of the project where the health check is performed. The value must be the same as the value of **project_id** in the token. The value contains a maximum of 255 characters.
project_id	No	String	Specifies the ID of the project to which the health check belongs. This parameter has the same meaning as **tenant_id**. The value must be the same as the value of **project_id** in the token.
name	No	String	Specifies the health check name. The value contains a maximum of 255 characters.
delay	Yes	Integer	Specifies the maximum time between health checks in the unit of second. The value ranges from **1** to **50**.
max_retries	Yes	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **OFFLINE** to **ONLINE**. The value ranges from **1** to **10**.
max_retries_down	No	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **ONLINE** to **OFFLINE**. The value ranges from **1** to **10**.
pool_id	Yes	String	Specifies the ID of the backend server group. Only one health check can be configured for each backend server group.
admin_state_up	No	Boolean	Specifies the administrative status of the health check. This parameter is reserved, and the default value is **true**.

Parameter	Mandatory	Type	Description
timeout	Yes	Integer	Specifies the health check timeout duration in the unit of second. The value ranges from **1** to **50**. **NOTE** You are advised to set the value less than that of parameter **delay**.
type	Yes	String	Specifies the health check protocol. The value can be **TCP**, **UDP_CONNECT**, or **HTTP**. The relationships between the health check protocol and the protocol used by the backend server group are as follows: • If the protocol of the backend server group is UDP, the parameter value can only be **UDP_CONNECT**. • If the protocol of the backend server group is TCP, the parameter value can be **TCP** or **HTTP**. • If the protocol of the backend server group is HTTP, the parameter value can be **TCP** or **HTTP**.
monitor_port	No	Integer	Specifies the health check port. The port number ranges from 1 to 65535. The value is left blank by default, indicating that the port of the backend server is used as the health check port.

Parameter	Mandatory	Type	Description
domain_name	No	String	Specifies the domain name of HTTP requests during the health check. This parameter is valid only when the value of **type** is set to **HTTP**. The value is left blank by default, indicating that the private IP address of the load balancer is used as the destination address of HTTP requests. The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter, for example, **www.test.com**. The value contains a maximum of 100 characters.
url_path	No	String	Specifies the HTTP request path for the health check. The default value is **/**, and the value must start with a slash (/). This parameter is valid only when the value of **type** is set to **HTTP**. An example value is **/test**. The value contains a maximum of 80 characters.
expected_codes	No	String	Specifies the expected HTTP status code. The following options are available: A single value, such as **200** A list of values, such as **200,202** A value range, such as **200–204** This parameter is valid only when the value of **type** is set to **HTTP**. The value contains a maximum of 64 characters. **NOTE** This parameter is reserved.

Parameter	Mandatory	Type	Description
http_method	No	String	Specifies the HTTP request method. The default value is **GET**. The value can be **GET**, **HEAD**, **POST**, **PUT**, **DELETE**, **TRACE**, **OPTIONS**, **CONNECT**, or **PATCH**. This parameter is valid only when the value of **type** is set to **HTTP**. **NOTE** This parameter is reserved.

Response

Table 10-120 Response parameters

Parameter	Type	Description
healthmonitor	Object	Specifies the health check. For details, see **Table 10-121**.

Table 10-121 healthmonitor parameter description

Parameter	Type	Description
id	String	Specifies the health check ID.
tenant_id	String	Specifies the ID of the project where the health check is performed.
project_id	String	Specifies the ID of the project to which the health check belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the health check name.
delay	Integer	Specifies the maximum time between health checks in the unit of second. The value ranges from **1** to **50**.
max_retries	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **OFFLINE** to **ONLINE**. The value ranges from **1** to **10**.
max_retries_down	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **ONLINE** to **OFFLINE**. The value ranges from **1** to **10**.

Parameter	Type	Description
pools	Array	Specifies the ID of the backend server group associated with the health check. For details, see Table 10-122.
admin_state_up	Boolean	Specifies the administrative status of the health check. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
timeout	Integer	Specifies the health check timeout duration in the unit of second. The value ranges from **1** to **50**. **NOTE** You are advised to set the value less than that of parameter **delay**.
type	String	Specifies the health check protocol. The value can be **TCP**, **UDP_CONNECT**, or **HTTP**. The relationships between the value of this parameter and the protocol of the backend server group are as follows: • If the protocol of the backend server group is UDP, the parameter value can only be **UDP_CONNECT**. • If the protocol of the backend server group is TCP, the parameter value can be **TCP** or **HTTP**. • If the protocol of the backend server group is HTTP, the parameter value can be **TCP** or **HTTP**.
monitor_port	Integer	Specifies the health check port. The port number ranges from 1 to 65535. The value is left blank by default, indicating that the port of the backend server is used as the health check port.

Parameter	Type	Description
expected_codes	String	Specifies the expected HTTP status code. The following options are available: A single value, such as **200** A list of values, such as **200,202** A value range, such as **200–204** This parameter is valid only when the value of **type** is set to **HTTP**. Currently, this parameter is not supported and is fixed at **200**.
domain_name	String	Specifies the domain name of HTTP requests during the health check. This parameter is valid only when the value of **type** is set to **HTTP**. The value is left blank by default, indicating that the private IP address of the load balancer is used as the destination address of HTTP requests. The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter, for example, **www.test.com**.
url_path	String	Specifies the HTTP request path for the health check. The default value is **/**, and the value must start with a slash (/). This parameter is valid only when the value of **type** is set to **HTTP**. An example value is **/test**.
http_method	String	Specifies the HTTP request method. The default value is **GET**. The value can be **GET**, **HEAD**, **POST**, **PUT**, **DELETE**, **TRACE**, **OPTIONS**, **CONNECT**, or **PATCH**. This parameter is valid only when the value of **type** is set to **HTTP**. **NOTE** This parameter is reserved.

Table 10-122 pools parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated backend server group.

Example Request

- Example request: Configuring a health check

```
POST https://{Endpoint}/v2.0/lbaas/healthmonitors

{
  "healthmonitor": {
    "admin_state_up": true,
    "pool_id": "bb44bffb-05d9-412c-9d9c-b189d9e14193",
    "domain_name": "www.test.com",
    "delay": 10,
    "max_retries": 10,
    "max_retries_down": 5,
    "timeout": 10,
    "type": "HTTP"
  }
}
```

Example Response

- Example response

```
{
  "healthmonitor": {
    "name": "",
    "admin_state_up": true,
    "tenant_id": "145483a5107745e9b3d80f956713e6a3",
    "project_id": "145483a5107745e9b3d80f956713e6a3",
    "domain_name": "www.test.com",
    "delay": 10,
    "max_retries": 10,
    "expected_codes": "200",
    "max_retries_down": 5,
    "http_method": "GET",
    "timeout": 10,
    "pools": [
      {
        "id": "bb44bffb-05d9-412c-9d9c-b189d9e14193"
      }
    ],
    "url_path": "/",
    "type": "HTTP",
    "id": "2dca3867-98c5-4cde-8f2c-b89ae6bd7e36",
    "monitor_port": 112
  }
}
```

Status Code

For details, see **Status Codes**.

10.1.5.2 Querying Health Checks

Function

This API is used to query the health checks. Filter query and pagination query are supported. Unless otherwise specified, exact match is applied.

URI

GET /v2.0/lbaas/healthmonitors

Constraints

Parameters **marker**, **limit**, and **page_reverse** are used for pagination query. Parameters **marker** and **page_reverse** take effect only when they are used together with parameter **limit**.

Request

Table 10-123 Parameter description

Parameter	Mandatory	Type	Description
marker	No	String	Specifies the ID of the health check from which pagination query starts, that is, the ID of the last health check on the previous page. This parameter must be used together with **limit**.
limit	No	Integer	Specifies the number of health checks on each page. If this parameter is not set, all health checks are queried by default.
page_reverse	No	Boolean	Specifies the page direction. The value can be **true** or **false**, and the default value is **false**. The last page in the list requested with **page_reverse** set to **false** will not contain the "next" link, and the last page in the list requested with **page_reverse** set to **true** will not contain the "previous" link. This parameter must be used together with **limit**.
id	No	String	Specifies the health check ID.
tenant_id	No	String	Specifies the ID of the project where the health check is performed. The value contains a maximum of 255 characters.
project_id	No	String	Specifies the ID of the project to which the health check belongs. This parameter has the same meaning as **tenant_id**.
name	No	String	Specifies the health check name. The value contains a maximum of 255 characters.
delay	No	Integer	Specifies the maximum time between health checks in the unit of second. The value ranges from **1** to **50**.

Parameter	Mandatory	Type	Description
max_retries	No	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **OFFLINE** to **ONLINE**. The value ranges from **1** to **10**.
max_retries_down	No	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **ONLINE** to **OFFLINE**. The value ranges from **1** to **10**.
admin_state_up	No	Boolean	Specifies the administrative status of the health check. This parameter is reserved, and the default value is **true**.
timeout	No	Integer	Specifies the health check timeout duration in the unit of second. The value ranges from **1** to **50**. **NOTE** You are advised to set the value less than that of parameter **delay**.
type	No	String	Specifies the health check protocol. The value can be **TCP**, **UDP_CONNECT**, or **HTTP**.
monitor_port	No	Integer	Specifies the port used for the health check. The value is left blank by default, indicating that the port of the backend server is used as the health check port.
expected_codes	No	String	Specifies the expected HTTP status code. The following options are available: A single value, such as **200** A list of values, such as **200,202** A value range, such as **200–204** This parameter is valid only when the value of **type** is set to **HTTP**. The value contains a maximum of 64 characters. **NOTE** This parameter is reserved.

Parameter	Mandatory	Type	Description
domain_name	No	String	Specifies the domain name of HTTP requests during the health check. This parameter is valid only when the value of **type** is set to **HTTP**. The value is left blank by default, indicating that the private IP address of the load balancer is used as the destination address of HTTP requests. The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter, for example, **www.test.com**. The value contains a maximum of 100 characters.
url_path	No	String	Specifies the HTTP request path for the health check. The default value is **/**, and the value must start with a slash (/). This parameter is valid only when the value of **type** is set to **HTTP**. An example value is **/test**. The value contains a maximum of 80 characters.
http_method	No	String	Specifies the HTTP request method. The default value is **GET**. The value can be **GET**, **HEAD**, **POST**, **PUT**, **DELETE**, **TRACE**, **OPTIONS**, **CONNECT**, or **PATCH**. This parameter is valid only when the value of **type** is set to **HTTP**. **NOTE** This parameter is reserved.

Response

Table 10-124 Response parameters

Parameter	Type	Description
healthmonitors	Array	Lists the health checks. For details, see **Table 10-125**.

Parameter	Type	Description
healthmonitors_links	Array	Provides links to the previous or next page during pagination query, respectively. This parameter exists only in the response body of pagination query. For details, see **Table 10-127**.

Table 10-125 healthmonitors parameter description

Parameter	Type	Description
id	String	Specifies the health check ID.
tenant_id	String	Specifies the ID of the project where the health check is performed.
project_id	String	Specifies the ID of the project to which the health check belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the health check name. The value contains a maximum of 255 characters.
delay	Integer	Specifies the maximum time between health checks in the unit of second. The value ranges from **1** to **50**.
max_retries	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **OFFLINE** to **ONLINE**. The value ranges from **1** to **10**.
max_retries_down	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **ONLINE** to **OFFLINE**. The value ranges from **1** to **10**.
pools	Array	Lists the IDs of backend server groups associated with the health check.
admin_state_up	Boolean	Specifies the administrative status of the health check. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled

Parameter	Type	Description
timeout	Integer	Specifies the health check timeout duration in the unit of second. The value ranges from **1** to **50**. **NOTE** You are advised to set the value less than that of parameter **delay**.
type	String	Specifies the health check protocol. The value can be **TCP**, **UDP_CONNECT**, or **HTTP**.
monitor_port	Integer	Specifies the health check port. The port number ranges from 1 to 65535. The value is left blank by default, indicating that the port of the backend server is used as the health check port.
expected_codes	String	Specifies the expected HTTP status code. The following options are available: A single value, such as **200** A list of values, such as **200,202** A value range, such as **200–204** This parameter is valid only when the value of **type** is set to **HTTP**. The value contains a maximum of 64 characters.
domain_name	String	Specifies the domain name of HTTP requests during the health check. This parameter is valid only when the value of **type** is set to **HTTP**. The value is left blank by default, indicating that the private IP address of the load balancer is used as the destination address of HTTP requests. The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter, for example, **www.test.com**. The value contains a maximum of 100 characters.

Parameter	Type	Description
url_path	String	Specifies the HTTP request path for the health check. The default value is **/**, and the value must start with a slash (/). This parameter is valid only when the value of **type** is set to **HTTP**. An example value is **/test**. The value contains a maximum of 80 characters.
http_method	String	Specifies the HTTP request method. The default value is **GET**. The value can be **GET**, **HEAD**, **POST**, **PUT**, **DELETE**, **TRACE**, **OPTIONS**, **CONNECT**, or **PATCH**. This parameter is valid only when the value of **type** is set to **HTTP**. **NOTE** This parameter is reserved.

Table 10-126 pools parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated backend server group.

Table 10-127 healthmonitors_links parameter description

Parameter	Type	Description
href	String	Provides links to the previous or next page during pagination query, respectively.
rel	String	Specifies the prompt of the previous or next page. The value can be **next** or **previous**. The value **next** indicates the href containing the URL of the next page, and **previous** indicates the href containing the URL of the previous page.

Example Request

- Example request 1: Querying all health checks
  GET https://{Endpoint}/v2.0/lbaas/healthmonitors
- Example request 2: Querying HTTP health checks
  GET https://{Endpoint}/v2.0/lbaas/healthmonitors?type=HTTP

Example Response

- Example response 1

```
{
   "healthmonitors": [
      {
         "monitor_port": null,
         "name": "",
         "admin_state_up": true,
         "tenant_id": "601240b9c5c94059b63d484c92cfe308",
         "project_id": "601240b9c5c94059b63d484c92cfe308",
         "domain_name": null,
         "delay": 5,

         "max_retries": 3,
         "max_retries_down": 5,
         "http_method": "GET",
         "timeout": 10,
         "pools": [
            {
               "id": "caef8316-6b65-4676-8293-cf41fb63cc2a"
            }
         ],
         "url_path": "/",
         "type": "HTTP",
         "id": "1b587819-d619-49c1-9101-fe72d8b361ef"
      }
   ]
}
```

- Example response 2

```
{
   "healthmonitors": [
      {
         "monitor_port": null,
         "name": "",
         "admin_state_up": true,
         "tenant_id": "601240b9c5c94059b63d484c92cfe308",
         "project_id": "601240b9c5c94059b63d484c92cfe308",
         "domain_name": null,
         "delay": 5,
         "expected_codes": "200-204,300-302,401",
         "max_retries": 3,
         "max_retries_down": 5,
         "http_method": "GET",
         "timeout": 10,
         "pools": [
            {
               "id": "caef8316-6b65-4676-8293-cf41fb63cc2a"
            }
         ],
         "url_path": "/",
         "type": "HTTP",
         "id": "1b587819-d619-49c1-9101-fe72d8b361ef"
      }
   ]
}
```

Status Code

For details, see **Status Codes**.

10.1.5.3 Querying Details of a Health Check

Function

This API is used to query details about a health check using its iD.

URI

GET /v2.0/lbaas/healthmonitors/{healthmonitor_id}

Table 10-128 Parameter description

Parameter	Mandatory	Type	Description
healthmonitor_id	Yes	String	Specifies the health check ID.

Request

None

Response

Table 10-129 Response parameters

Parameter	Type	Description
healthmonitor	Object	Specifies the health check. For details, see **Table 10-130**.

Table 10-130 healthmonitor parameter description

Parameter	Type	Description
id	String	Specifies the health check ID.
tenant_id	String	Specifies the ID of the project where the health check is performed.
project_id	String	Specifies the ID of the project to which the health check belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the health check name.
delay	Integer	Specifies the maximum time between health checks in the unit of second. The value ranges from **1** to **50**.

Parameter	Type	Description
max_retries	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **OFFLINE** to **ONLINE**. The value ranges from **1** to **10**.
max_retries_down	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **ONLINE** to **OFFLINE**. The value ranges from **1** to **10**.
pools	Array	Specifies the ID of the backend server group associated with the health check. For details, see **Table 10-122**.
admin_state_up	Boolean	Specifies the administrative status of the health check. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
timeout	Integer	Specifies the health check timeout duration in the unit of second. The value ranges from **1** to **50**. **NOTE** You are advised to set the value less than that of parameter **delay**.
type	String	Specifies the health check protocol. The value can be **TCP**, **UDP_CONNECT**, or **HTTP**. The relationships between the value of this parameter and the protocol of the backend server group are as follows: • If the protocol of the backend server group is UDP, the parameter value can only be **UDP_CONNECT**. • If the protocol of the backend server group is TCP, the parameter value can be **TCP** or **HTTP**. • If the protocol of the backend server group is HTTP, the parameter value can be **TCP** or **HTTP**.
monitor_port	Integer	Specifies the health check port. The port number ranges from 1 to 65535. The value is left blank by default, indicating that the port of the backend server is used as the health check port.

Parameter	Type	Description
expected_codes	String	Specifies the expected HTTP status code. The following options are available: A single value, such as **200** A list of values, such as **200,202** A value range, such as **200–204** This parameter is valid only when the value of **type** is set to **HTTP**. Currently, this parameter is not supported and is fixed at **200**.
domain_name	String	Specifies the domain name of HTTP requests during the health check. This parameter is valid only when the value of **type** is set to **HTTP**. The value is left blank by default, indicating that the private IP address of the load balancer is used as the destination address of HTTP requests. The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter, for example, **www.test.com**.
url_path	String	Specifies the HTTP request path for the health check. The default value is **/**, and the value must start with a slash (/). This parameter is valid only when the value of **type** is set to **HTTP**. An example value is **/test**.
http_method	String	Specifies the HTTP request method. The default value is **GET**. The value can be **GET**, **HEAD**, **POST**, **PUT**, **DELETE**, **TRACE**, **OPTIONS**, **CONNECT**, or **PATCH**. This parameter is valid only when the value of **type** is set to **HTTP**. **NOTE** This parameter is reserved.

Table 10-131 pools parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated backend server group.

Example Request

- Example request: Querying details of a health check
  ```
  GET https://{Endpoint}/v2.0/lbaas/healthmonitors/b7633ade-24dc-4d72-8475-06aa22be5412
  ```

Example Response

- Example response
  ```
  {
    "healthmonitor": {
      "name": "",
      "admin_state_up": true,
      "tenant_id": "145483a5107745e9b3d80f956713e6a3",
      "project_id": "145483a5107745e9b3d80f956713e6a3",
      "domain_name": null,
      "delay": 10,
      "expected_codes": "200-204,300-302,401",
      "max_retries": 10,
      "max_retries_down": 5,
      "http_method": "GET",
      "timeout": 10,
      "pools": [
        {
          "id": "bb44bffb-05d9-412c-9d9c-b189d9e14193"
        }
      ],
      "url_path": "/",
      "type": "HTTP",
      "id": "61c24cba-19bb-45c1-a013-7565e5f98872",
      "monitor_port": 112
    }
  }
  ```

Status Code

For details, see **Status Codes**.

10.1.5.4 Updating a Health Check

Function

This API is used to update a health check.

Constraints

If **provisioning_status** of the load balancer for which the health check is configured is not **ACTIVE**, the health check cannot be updated.

URI

PUT /v2.0/lbaas/healthmonitors/{healthmonitor_id}

Table 10-132 Parameter description

Parameter	Mandatory	Type	Description
healthmonitor_id	Yes	String	Specifies the health check ID.

Request

Table 10-133 Parameter description

Parameter	Mandatory	Type	Description
healthmonitor	Yes	Object	Specifies the health check. For details, see **Table 10-134**.

Table 10-134 healthmonitor parameter description

Parameter	Mandatory	Type	Description
name	No	String	Specifies the health check name. The value contains a maximum of 255 characters.
delay	No	Integer	Specifies the maximum time between health checks in the unit of second. The value ranges from **1** to **50**.
max_retries	No	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **OFFLINE** to **ONLINE**. The value ranges from **1** to **10**.
max_retries_down	No	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **ONLINE** to **OFFLINE**. The value ranges from **1** to **10**.
admin_state_up	No	Boolean	Specifies the administrative status of the health check. This parameter is reserved, and the default value is **true**.
timeout	No	Integer	Specifies the health check timeout duration in the unit of second. The value ranges from **1** to **50**. **NOTE** You are advised to set the value less than that of parameter **delay**.
type	No	String	Specifies the health check protocol. The value can be **TCP**, **UDP_CONNECT**, or **HTTP**.

Parameter	Mandatory	Type	Description
monitor_port	No	Integer	Specifies the health check port. The port number ranges from 1 to 65535. The value is left blank by default, indicating that the port of the backend server is used as the health check port.
expected_codes	No	String	Specifies the expected HTTP status code. The following options are available: A single value, such as **200** A list of values, such as **200,202** A value range, such as **200–204** This parameter is valid only when the value of **type** is set to **HTTP**.
domain_name	No	String	Specifies the domain name of HTTP requests during the health check. This parameter is valid only when the value of **type** is set to **HTTP**. The value is left blank by default, indicating that the private IP address of the load balancer is used as the destination address of HTTP requests. The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter, for example, **www.test.com**. The value contains a maximum of 100 characters.
url_path	No	String	Specifies the HTTP request path for the health check. The default value is **/**, and the value must start with a slash (/). This parameter is valid only when the value of **type** is set to **HTTP**. An example value is **/test**. The value contains a maximum of 80 characters.

Parameter	Mandatory	Type	Description
http_method	No	String	Specifies the HTTP request method. The default value is **GET**. The value can be **GET**, **HEAD**, **POST**, **PUT**, **DELETE**, **TRACE**, **OPTIONS**, **CONNECT**, or **PATCH**. This parameter is valid only when the value of **type** is set to **HTTP**. **NOTE** This parameter is reserved.

Response

Table 10-135 Response parameters

Parameter	Type	Description
healthmonitor	Object	Specifies the health check. For details, see **Table 10-136**.

Table 10-136 healthmonitor parameter description

Parameter	Type	Description
id	String	Specifies the health check ID.
tenant_id	String	Specifies the ID of the project where the health check is performed.
project_id	String	Specifies the ID of the project to which the health check belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the health check name.
delay	Integer	Specifies the maximum time between health checks in the unit of second. The value ranges from **1** to **50**.
max_retries	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **OFFLINE** to **ONLINE**. The value ranges from **1** to **10**.
max_retries_down	Integer	Specifies the number of consecutive health checks when the health check result of a backend server changes from **ONLINE** to **OFFLINE**. The value ranges from **1** to **10**.

Parameter	Type	Description
pools	Array	Specifies the ID of the backend server group associated with the health check. For details, see Table 10-122.
admin_state_up	Boolean	Specifies the administrative status of the health check. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
timeout	Integer	Specifies the health check timeout duration in the unit of second. The value ranges from **1** to **50**. **NOTE** You are advised to set the value less than that of parameter **delay**.
type	String	Specifies the health check protocol. The value can be **TCP**, **UDP_CONNECT**, or **HTTP**. The relationships between the value of this parameter and the protocol of the backend server group are as follows: • If the protocol of the backend server group is UDP, the parameter value can only be **UDP_CONNECT**. • If the protocol of the backend server group is TCP, the parameter value can be **TCP** or **HTTP**. • If the protocol of the backend server group is HTTP, the parameter value can be **TCP** or **HTTP**.
monitor_port	Integer	Specifies the health check port. The port number ranges from 1 to 65535. The value is left blank by default, indicating that the port of the backend server is used as the health check port.

Parameter	Type	Description
expected_codes	String	Specifies the expected HTTP status code. The following options are available: A single value, such as **200** A list of values, such as **200,202** A value range, such as **200–204** This parameter is valid only when the value of **type** is set to **HTTP**. Currently, this parameter is not supported and is fixed at **200**.
domain_name	String	Specifies the domain name of HTTP requests during the health check. This parameter is valid only when the value of **type** is set to **HTTP**. The value is left blank by default, indicating that the private IP address of the load balancer is used as the destination address of HTTP requests. The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter, for example, **www.test.com**.
url_path	String	Specifies the HTTP request path for the health check. The default value is **/**, and the value must start with a slash (/). This parameter is valid only when the value of **type** is set to **HTTP**. An example value is **/test**.
http_method	String	Specifies the HTTP request method. The default value is **GET**. The value can be **GET**, **HEAD**, **POST**, **PUT**, **DELETE**, **TRACE**, **OPTIONS**, **CONNECT**, or **PATCH**. This parameter is valid only when the value of **type** is set to **HTTP**. **NOTE** This parameter is reserved.

Table 10-137 pools parameter description

Parameter	Type	Description
id	String	Specifies the ID of the associated backend server group.

Example Request

- Example request: Updating a health check

```
PUT https://{Endpoint}/v2.0/lbaas/healthmonitors/b7633ade-24dc-4d72-8475-06aa22be5412

{
  "healthmonitor": {
    "delay": 15,
    "name": "health-xx",
    "timeout": 12
  }
}
```

Example Response

- Example response

```
{
  "healthmonitor": {
    "name": "health-xx",
    "admin_state_up": true,
    "tenant_id": "145483a5107745e9b3d80f956713e6a3",
    "project_id": "145483a5107745e9b3d80f956713e6a3",
    "domain_name": null,
    "delay": 15,
    "expected_codes": "200",
    "max_retries": 10,
    "max_retries_down": 5,
    "http_method": "GET",
    "timeout": 12,
    "pools": [
      {
        "id": "bb44bffb-05d9-412c-9d9c-b189d9e14193"
      }
    ],
    "url_path": "/",
    "type": "HTTP",
    "id": "2dca3867-98c5-4cde-8f2c-b89ae6bd7e36",
    "monitor_port": 112
  }
}
```

Status Code

For details, see **Status Codes**.

10.1.5.5 Deleting a Health Check

Function

This API is used to delete a health check.

Constraints

If **provisioning_status** of the load balancer for which the health check is configured is not **ACTIVE**, the health check cannot be deleted.

URI

DELETE /v2.0/lbaas/healthmonitors/{healthmonitor_id}

Table 10-138 Parameter description

Parameter	Mandatory	Type	Description
healthmonitor_id	Yes	String	Specifies the health check ID.

Request

None

Response

None

Example Request

- Example request: Deleting a health check
  DELETE https://{Endpoint}/v2.0/lbaas/healthmonitors/b7633ade-24dc-4d72-8475-06aa22be5412

Example Response

- Example response

  None

Status Code

For details, see **Status Codes**.

10.1.6 Forwarding Policy

10.1.6.1 Adding a Forwarding Policy

Function

This API is used to add a forwarding policy. The listener and forwarding policy determine how traffic is forwarded to backend servers.

- By matching the URL or domain name specified in the forwarding policy when **action** is set to **REDIRECT_TO_POOL**, the load balancer distributes the traffic to backend servers in a specific backend server group.
- When **action** is set to **REDIRECT_TO_LISTENER**, the HTTP listener is redirected to an HTTPS listener, and requests are routed by the HTTPS listener.

Constraints

Currently, only redirects from an HTTP listener to an HTTPS listener are supported. When **action** is set to **REDIRECT_TO_LISTENER**, the listener specified by **listener_id** can only be an HTTP listener, and the listener specified by **redirect_listener_id** can only be an HTTPS listener.

The load balancer of the HTTPS listener to which traffic is redirected must be the same as that of the HTTP listener.

URI

POST /v2.0/lbaas/l7policies

Request

Table 10-139 Parameter description

Parameter	Mandatory	Type	Description
l7policy	Yes	Object	Specifies the forwarding policy. For details, see **Table 10-140**.

Table 10-140 l7policy parameter description

Parameter	Mandatory	Type	Description
tenant_id	No	String	Specifies the ID of the project where the forwarding policy is used. The value must be the same as the value of **tenant_id** in the token. The value contains a maximum of 255 characters.
project_id	No	String	Specifies the ID of the project to which the forwarding policy belongs. This parameter has the same meaning as **tenant_id**. The value must be the same as the value of **project_id** in the token.
name	No	String	Specifies the forwarding policy name. The value contains a maximum of 255 characters.
admin_state_up	No	Boolean	Specifies the administrative status of the forwarding policy. This parameter is reserved, and the default value is **true**.

Parameter	Mandatory	Type	Description
description	No	String	Provides supplementary information about the forwarding policy. The value contains a maximum of 255 characters.
listener_id	Yes	String	Specifies the ID of the listener to which the forwarding policy is added. • When **action** is set to **REDIRECT_TO_POOL**, forwarding policies can be added to a listener with **protocol** set to **HTTP** or **TERMINATED_HTTPS**. • When **action** is set to **REDIRECT_TO_LISTENER**, forwarding policies can be added to a listener with **protocol** set to **HTTP**.
action	Yes	String	Specifies whether requests are forwarded to another backend server group or redirected to an HTTPS listener. The value can be one of the following: • **REDIRECT_TO_POOL**: Requests are forwarded to the backend server group specified by **redirect_pool_id**. • **REDIRECT_TO_LISTENER**: Requests are redirected from the HTTP listener specified by **listener_id** to the HTTPS listener specified by **redirect_listener_id**.

Parameter	Mandatory	Type	Description
redirect_pool_id	No	String	Specifies the ID of the backend server group to which traffic is forwarded. The default value is **null**. This parameter is mandatory when **action** is set to **REDIRECT_TO_POOL**. This parameter cannot be specified when **action** is set to **REDIRECT_TO_LISTENER**. The backend server group must meet the following requirements: • Cannot be the default backend server group of the listener. • Cannot be the backend server group used by forwarding policies of other listeners.
redirect_listener_id	No	String	Specifies the ID of the listener to which the traffic is redirected. The default value is **null**. This parameter cannot be specified when **action** is set to **REDIRECT_TO_POOL**. This parameter is mandatory when **action** is set to **REDIRECT_TO_LISTENER**, and the listener: • Can only be an HTTPS listener. • Can only be a listener of the same load balancer.
redirect_url	No	String	Specifies the URL to which traffic is redirected. The default value is **null**. This parameter is reserved. The value contains a maximum of 255 characters.
position	No	Integer	Specifies the forwarding priority. The value ranges from **1** to **100**. The default value is **100**. This parameter is reserved.

Parameter	Mandatory	Type	Description
rules	No	Array	Lists the forwarding rules of the forwarding policy. For details, see **Table 10-141**. The list contains a maximum of two rules, and the **type** parameter of each rule must be unique.

Table 10-141 rules parameter description

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Specifies the administrative status of the forwarding rule. This parameter is reserved, and the default value is **true**.
type	Yes	String	Specifies the match type of a forwarding rule. The value range varies depending on the protocol of the backend server group: • **HOST_NAME**: matches the domain name in the request. • **PATH**: matches the path in the request. The match type of forwarding rules in a forwarding policy must be unique.
compare_type	Yes	String	Specifies the match mode. The options are as follows: When **type** is set to **HOST_NAME**, the value of this parameter can only be the following: • **EQUAL_TO**: indicates exact match. When **type** is set to **PATH**, the value of this parameter can be one of the following: • **REGEX**: indicates regular expression match. • **STARTS_WITH**: indicates prefix match. • **EQUAL_TO**: indicates exact match.

Parameter	Mandatory	Type	Description
invert	No	Boolean	Specifies whether reverse matching is supported. The value can be **true** or **false**. The default value is **false**. This parameter is reserved.
key	No	String	Specifies the key of the match content. The default value is **null**. This parameter is reserved.
value	Yes	String	Specifies the value of the match content. The value cannot contain spaces. • When **type** is set to **HOST_NAME**, the value can contain a maximum of 100 characters that contain only letters, digits, hyphens (-), and periods (.), and must start with a letter or digit. • When **type** is set to **PATH**, the value can contain a maximum of 128 characters. When **compare_type** is set to **STARTS_WITH** or **EQUAL_TO**, the value must start with a slash (/) and can contain only letters, digits, and special characters _~';@^-%#&$.*+?,=!:|\/()[]{}

Response

Table 10-142 Response parameters

Parameter	Type	Description
l7policy	Object	Specifies the forwarding policy. For details, see **Table 10-143**.

Table 10-143 l7policy parameter description

Parameter	Type	Description
id	String	Specifies the forwarding policy ID.
tenant_id	String	Specifies the ID of the project where the forwarding policy is used.

Parameter	Type	Description
project_id	String	Specifies the ID of the project to which the forwarding policy belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the forwarding policy name.
admin_state_up	Boolean	Specifies the administrative status of the forwarding policy. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
description	String	Provides supplementary information about the forwarding policy.
listener_id	String	Specifies the ID of the listener to which the forwarding policy is added.
action	String	Specifies whether requests are forwarded to another backend server group or redirected to an HTTPS listener. The value can be one of the following: • **REDIRECT_TO_POOL**: Requests are forwarded to the backend server group specified by **redirect_pool_id**. • **REDIRECT_TO_LISTENER**: Requests are redirected from the HTTP listener specified by **listener_id** to the HTTPS listener specified by **redirect_listener_id**.
redirect_pool_id	String	Specifies the ID of the backend server group to which traffic is forwarded.
redirect_listener_id	String	Specifies the ID of the listener to which the traffic is redirected.
redirect_url	String	Specifies the URL to which traffic is redirected. This parameter is reserved.
rules	Array	Lists the forwarding rules of the forwarding policy. For details, see **Table 10-144**.
position	Integer	Specifies the forwarding priority. The value ranges from **1** to **100**. The default value is **100**. This parameter is reserved.

Parameter	Type	Description
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the forwarding policy.

Table 10-144 rules parameter description

Parameter	Type	Description
id	String	Lists the IDs of the forwarding rules in the forwarding policy.

Example Request

- Example request 1: Adding a forwarding policy

```
POST https://{Endpoint}/v2.0/lbaas/l7policies

{
    "l7policy": {
        "name": "niubiao_yaqing_api-2",
        "listener_id": "3e24a3ca-11e5-4aa3-abd4-61ba0a8a18f1",
        "action": "REDIRECT_TO_POOL",
        "redirect_pool_id": "6460f13a-76de-43c7-b776-4fefc06a676e",
        "rules": [
            {
                "type": "PATH",
                "compare_type": "EQUAL_TO",
                "value": "/test"
            },
            {
                "type": "HOST_NAME",
                "compare_type": "EQUAL_TO",
                "value": "www.test.com"
            }
        ]
    }
}
```

Example Response

- Example response 1

```
{
    "l7policy": {
        "redirect_pool_id": "6460f13a-76de-43c7-b776-4fefc06a676e",
        "description": "",
        "admin_state_up": true,
        "rules": [
            {
                "id": "742600d9-2a14-4808-af69-336883dbb590"
            },
            {
                "id": "3251ed77-0d52-412b-9310-733636bb3fbf"
            }
        ],
        "tenant_id": "573d73c9f90e48d0bddfa0eb202b25c2",
        "listener_id": "3e24a3ca-11e5-4aa3-abd4-61ba0a8a18f1",
        "redirect_url": null,
```



```
    "redirect_listener_id": null,
    "action": "REDIRECT_TO_POOL",
    "position": 100,
    "provisioning_status": "ACTIVE",
    "project_id": "573d73c9f90e48d0bddfa0eb202b25c2",
    "id": "65d6e115-f179-4bcd-9bbb-1484e5f8ee81",
    "name": "niubiao_yaqing-_api-2"
  }
}
```


Status Code

For details, see **Status Codes**.

10.1.6.2 Querying Forwarding Policies

Function

This API is used to query the forwarding policies. Filter query and pagination query are supported. Unless otherwise specified, exact match is applied.

Constraints

Parameters **marker**, **limit**, and **page_reverse** are used for pagination query. Parameters **marker** and **page_reverse** take effect only when they are used together with parameter **limit**.

URI

GET /v2.0/lbaas/l7policies

Request

Table 10-145 Parameter description

Parameter	Mandatory	Type	Description
marker	No	String	Specifies the ID of the forwarding policy from which pagination query starts, that is, the ID of the last forwarding policy on the previous page. This parameter must be used together with **limit**.
limit	No	Integer	Specifies the number of forwarding policies on each page. If this parameter is not set, all forwarding policies are queried by default.

Parameter	Mandatory	Type	Description
page_reverse	No	Boolean	Specifies the page direction. The value can be **true** or **false**, and the default value is **false**. The last page in the list requested with **page_reverse** set to **false** will not contain the "next" link, and the last page in the list requested with **page_reverse** set to **true** will not contain the "previous" link. This parameter must be used together with **limit**.
id	No	String	Specifies the forwarding policy ID.
tenant_id	No	String	Specifies the ID of the project where the forwarding policy is used. The value contains a maximum of 255 characters.
project_id	No	String	Specifies the ID of the project to which the forwarding policy belongs. This parameter has the same meaning as **tenant_id**.
name	No	String	Specifies the forwarding policy name. The value contains a maximum of 255 characters.
admin_state_up	No	Boolean	Specifies the administrative status of the forwarding policy. This parameter is reserved, and the default value is **true**.
description	No	String	Provides supplementary information about the forwarding policy. The value contains a maximum of 255 characters.
listener_id	No	String	Specifies the ID of the listener to which the forwarding policy is added.

Parameter	Mandatory	Type	Description
action	No	String	Specifies whether requests are forwarded to another backend server group or redirected to an HTTPS listener. The value can be one of the following: • **REDIRECT_TO_POOL**: Requests are forwarded to the backend server group specified by **redirect_pool_id**. • **REDIRECT_TO_LISTENER**: Requests are redirected from the HTTP listener specified by **listener_id** to the HTTPS listener specified by **redirect_listener_id**.
redirect_pool_id	No	String	Specifies the ID of the backend server group to which traffic is forwarded.
redirect_listener_id	No	String	Specifies the ID of the listener to which the traffic is redirected.
redirect_url	No	String	Specifies the URL to which traffic is redirected. This parameter is reserved. The value contains a maximum of 255 characters.
position	No	Integer	Specifies the forwarding priority. The value ranges from **1** to **100**. The default value is **100**. This parameter is reserved.
provisioning_status	No	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the forwarding policy.
display_all_rules	No	Boolean	Specifies whether to display all forwarding rules added to the forwarding policy. Value options: **false**: Forwarding rules will not be displayed, and only IDs are displayed. **true**: Forwarding rules will be displayed.

Response

Table 10-146 Response parameters

Parameter	Type	Description
l7policies	Array	Lists the forwarding policies. For details, see **Table 10-147**.
l7policies_links	Array	Provides links to the previous or next page during pagination query, respectively. This parameter exists only in the response body of pagination query. For details, see **Table 10-149**.

Table 10-147 l7policy parameter description

Parameter	Type	Description
id	String	Specifies the forwarding policy ID.
tenant_id	String	Specifies the ID of the project where the forwarding policy is used.
project_id	String	Specifies the ID of the project to which the forwarding policy belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the forwarding policy name.
admin_state_up	Boolean	Specifies the administrative status of the forwarding policy. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
description	String	Provides supplementary information about the forwarding policy.
listener_id	String	Specifies the ID of the listener to which the forwarding policy is added.

Parameter	Type	Description
action	String	Specifies whether requests are forwarded to another backend server group or redirected to an HTTPS listener. The value can be one of the following: • **REDIRECT_TO_POOL**: Requests are forwarded to the backend server group specified by **redirect_pool_id**. • **REDIRECT_TO_LISTENER**: Requests are redirected from the HTTP listener specified by **listener_id** to the HTTPS listener specified by **redirect_listener_id**.
redirect_pool_id	String	Specifies the ID of the backend server group to which traffic is forwarded.
redirect_listener_id	String	Specifies the ID of the listener to which the traffic is redirected.
redirect_url	String	Specifies the URL to which traffic is redirected. This parameter is reserved.
rules	Array	Lists the forwarding rules of the forwarding policy. For details, see **Table 10-144**.
position	Integer	Specifies the forwarding priority. The value ranges from **1** to **100**. The default value is **100**. This parameter is reserved.
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the forwarding policy.

Table 10-148 rules parameter description

Parameter	Type	Description
id	String	Lists the IDs of the forwarding rules in the forwarding policy.

Table 10-149 l7policies_links parameter description

Parameter	Type	Description
href	String	Provides links to the previous or next page during pagination query, respectively.

Parameter	Type	Description
rel	String	Specifies the prompt of the previous or next page. The value can be **next** or **previous**. The value **next** indicates the href containing the URL of the next page, and **previous** indicates the href containing the URL of the previous page.

Example Request

- Example request 1: Querying all forwarding policies
  ```
  GET https://{Endpoint}/v2.0/lbaas/l7policies
  ```
- Example request 2: Querying forwarding policies through which requests are forwarded to the backend server group
  ```
  GET https://{Endpoint}/v2.0/lbaas/l7policies?action=REDIRECT_TO_POOL
  ```

Example Response

- Example response 1
  ```
  {
     "l7policies": [
        {
           "redirect_pool_id": "431a03eb-81bb-408e-ae37-7ce19023692b",
           "redirect_listener_id": null,
           "description": "",
           "admin_state_up": true,
           "rules": [
              {
                 "id": "67d8a8fa-b0dd-4bd4-a85b-671db19b2ef3"
              },
              {
                 "id": "f02b3bca-69d2-4335-a3fa-a8054e996213"
              }
           ],
           "tenant_id": "a31d2bdcf7604c0faaddb058e1e08819",
           "project_id": "a31d2bdcf7604c0faaddb058e1e08819",
           "listener_id": "26058b64-6185-4e06-874e-4bd68b7633d0",
           "redirect_url": null,
           "action": "REDIRECT_TO_POOL",
           "position": 2,
           "provisioning_status": "ACTIVE",
           "id": "5ae0e1e7-5f0f-47a1-b39f-5d4c428a1586",
           "name": ""
        },
        {
           "redirect_pool_id": "59eebd7b-c68f-4f8a-aa7f-e062e84c0690",
           "redirect_listener_id": null,
           "description": "",
           "admin_state_up": true,
           "rules": [
              {
                 "id": "f4499f48-de3d-4efe-926d-926aa4d6aaf5"
              }
           ],
           "tenant_id": "a31d2bdcf7604c0faaddb058e1e08819",
           "project_id": "a31d2bdcf7604c0faaddb058e1e08819",
           "listener_id": "e1310063-00de-4867-ab55-ccac4d9db364",
           "redirect_url": null,
           "action": "REDIRECT_TO_POOL",
  ```



```
            "position": 1,
            "provisioning_status": "ACTIVE",
            "id": "6cfd9d89-1d7e-4d84-ae1f-a8c5ff126f72",
            "name": ""
        }
    ],
    "l7policies_links": [
        {
        "href": "https://{Endpoint}/v2.0/lbaas/l7policies/061f461c-c7cf-47ab-9583-09be5076cd09/rules?
marker=167c1a31-bc12-4c3d-9ad1-c9bf450df4ce&page_reverse=True",
        "rel": "previous"
        }
    ]
}
```


- Example response 2


```
{
    "l7policies": [
        {
            "redirect_pool_id": "431a03eb-81bb-408e-ae37-7ce19023692b",
            "redirect_listener_id": null,
            "description": "",
            "admin_state_up": true,
            "rules": [
                {
                    "id": "67d8a8fa-b0dd-4bd4-a85b-671db19b2ef3"
                },
                {
                    "id": "f02b3bca-69d2-4335-a3fa-a8054e996213"
                }
            ],
            "tenant_id": "a31d2bdcf7604c0faaddb058e1e08819",
            "project_id": "a31d2bdcf7604c0faaddb058e1e08819",
            "listener_id": "26058b64-6185-4e06-874e-4bd68b7633d0",
            "redirect_url": null,
            "action": "REDIRECT_TO_POOL",
            "position": 2,
            "provisioning_status": "ACTIVE",
            "id": "5ae0e1e7-5f0f-47a1-b39f-5d4c428a1586",
            "name": ""
        },
        {
            "redirect_pool_id": "59eebd7b-c68f-4f8a-aa7f-e062e84c0690",
            "redirect_listener_id": null,
            "description": "",
            "admin_state_up": true,
            "rules": [
                {
                    "id": "f4499f48-de3d-4efe-926d-926aa4d6aaf5"
                }
            ],
            "tenant_id": "a31d2bdcf7604c0faaddb058e1e08819",
            "project_id": "a31d2bdcf7604c0faaddb058e1e08819",
            "listener_id": "e1310063-00de-4867-ab55-ccac4d9db364",
            "redirect_url": null,
            "action": "REDIRECT_TO_POOL",
            "position": 1,
            "provisioning_status": "ACTIVE",
            "id": "6cfd9d89-1d7e-4d84-ae1f-a8c5ff126f72",
            "name": ""
        }
    ],
    "l7policies_links": [
        {
        "href": "https://{Endpoint}/v2.0/lbaas/l7policies/061f461c-c7cf-47ab-9583-09be5076cd09/rules?
marker=167c1a31-bc12-4c3d-9ad1-c9bf450df4ce&page_reverse=True",
        "rel": "previous"
        }
    ]
}
```


Status Code

For details, see **Status Codes**.

10.1.6.3 Querying Details of a Forwarding Policy

Function

This API is used to query details about a forwarding policy.

URI

GET /v2.0/lbaas/l7policies/{l7policy_id}

Table 10-150 Parameter description

Parameter	Mandatory	Type	Description
l7policy_id	Yes	String	Specifies the forwarding policy ID.

Request

None

Response

Table 10-151 Parameter description

Parameter	Type	Description
l7policy	Object	Specifies the forwarding policy. For details, see **Table 10-152**.

Table 10-152 l7policy parameter description

Parameter	Type	Description
id	String	Specifies the forwarding policy ID.
tenant_id	String	Specifies the ID of the project where the forwarding policy is used.
project_id	String	Specifies the ID of the project to which the forwarding policy belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the forwarding policy name.

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the forwarding policy. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
description	String	Provides supplementary information about the forwarding policy.
listener_id	String	Specifies the ID of the listener to which the forwarding policy is added.
action	String	Specifies whether requests are forwarded to another backend server group or redirected to an HTTPS listener. The value can be one of the following: • **REDIRECT_TO_POOL**: Requests are forwarded to the backend server group specified by **redirect_pool_id**. • **REDIRECT_TO_LISTENER**: Requests are redirected from the HTTP listener specified by **listener_id** to the HTTPS listener specified by **redirect_listener_id**.
redirect_pool_id	String	Specifies the ID of the backend server group to which traffic is forwarded.
redirect_listener_id	String	Specifies the ID of the listener to which the traffic is redirected.
redirect_url	String	Specifies the URL to which traffic is redirected. This parameter is reserved.
rules	Array	Lists the forwarding rules of the forwarding policy. For details, see **Table 10-144**.
position	Integer	Specifies the forwarding priority. The value ranges from **1** to **100**. The default value is **100**. This parameter is reserved.
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the forwarding policy.

Table 10-153 rules parameter description

Parameter	Type	Description
id	String	Lists the IDs of the forwarding rules in the forwarding policy.

Example Request

- Example request: Querying details of a forwarding policy
  GET https://{Endpoint}/v2.0/lbaas/l7policies/5ae0e1e7-5f0f-47a1-b39f-5d4c428a1586

Example Response

- Example response

```
{
    "l7policy": {
        "redirect_pool_id": "431a03eb-81bb-408e-ae37-7ce19023692b",
        "redirect_listener_id": null,
        "description": "",
        "admin_state_up": true,
        "rules": [
            {
                "id": "67d8a8fa-b0dd-4bd4-a85b-671db19b2ef3"
            },
            {
                "id": "f02b3bca-69d2-4335-a3fa-a8054e996213"
            }
        ],
        "tenant_id": "a31d2bdcf7604c0faaddb058e1e08819",
        "project_id": "a31d2bdcf7604c0faaddb058e1e08819",
        "listener_id": "26058b64-6185-4e06-874e-4bd68b7633d0",
        "redirect_url": null,
        "provisioning_status": "ACTIVE",
        "action": "REDIRECT_TO_POOL",
        "position": 1,
        "id": "5ae0e1e7-5f0f-47a1-b39f-5d4c428a1586",
        "name": "l7policy-garry-1"
    }
}
```

Status Code

For details, see **Status Codes**.

10.1.6.4 Updating a Forwarding Policy

Function

This API is used to update a forwarding policy. You can select another backend server group or redirect to another HTTPS listener.

URI

PUT /v2.0/lbaas/l7policies/{l7policy_id}

Table 10-154 Parameter description

Parameter	Mandatory	Type	Description
l7policy_id	Yes	Object	Specifies the forwarding policy ID.

Request

Table 10-155 Parameter description

Parameter	Mandatory	Type	Description
l7policy	Yes	Object	Specifies the forwarding policy. For details, see **Table 10-156**.

Table 10-156 l7policy parameter description

Parameter	Mandatory	Type	Description
name	No	String	Specifies the forwarding policy name. The value contains a maximum of 255 characters.
description	No	String	Provides supplementary information about the forwarding policy. The value contains a maximum of 255 characters.
redirect_pool_id	No	String	Specifies the ID of the backend server group to which traffic is forwarded. The default value is **null**. This parameter is mandatory when **action** is set to **REDIRECT_TO_POOL**. This parameter cannot be specified when **action** is set to **REDIRECT_TO_LISTENER**. The backend server group must meet the following requirements: • Cannot be the default backend server group of the listener. • Cannot be the backend server group used by forwarding policies of other listeners.

Parameter	Mandatory	Type	Description
redirect_listener_id	No	String	Specifies the ID of the listener to which the traffic is redirected. The default value is **null**. This parameter is mandatory when **action** is set to **REDIRECT_TO_LISTENER**. This parameter cannot be specified when **action** is set to **REDIRECT_TO_POOL**. The listener must meet the following requirements: • Can only be an HTTPS listener. • Can only be a listener of the same load balancer.
admin_state_up	No	Boolean	Specifies the administrative status of the forwarding policy. This parameter is reserved, and the default value is **true**.

Response

Table 10-157 Response parameters

Parameter	Mandatory	Type	Description
l7policy	Yes	Object	Specifies the forwarding policy. For details, see **Table 10-158**.

Table 10-158 l7policy parameter description

Parameter	Type	Description
id	String	Specifies the forwarding policy ID.
tenant_id	String	Specifies the ID of the project where the forwarding policy is used.
project_id	String	Specifies the ID of the project to which the forwarding policy belongs. This parameter has the same meaning as **tenant_id**.
name	String	Specifies the forwarding policy name.

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the forwarding policy. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
description	String	Provides supplementary information about the forwarding policy.
listener_id	String	Specifies the ID of the listener to which the forwarding policy is added.
action	String	Specifies whether requests are forwarded to another backend server group or redirected to an HTTPS listener. The value can be one of the following: • **REDIRECT_TO_POOL**: Requests are forwarded to the backend server group specified by **redirect_pool_id**. • **REDIRECT_TO_LISTENER**: Requests are redirected from the HTTP listener specified by **listener_id** to the HTTPS listener specified by **redirect_listener_id**.
redirect_pool_id	String	Specifies the ID of the backend server group to which traffic is forwarded.
redirect_listener_id	String	Specifies the ID of the listener to which the traffic is redirected.
redirect_url	String	Specifies the URL to which traffic is redirected. This parameter is reserved.
rules	Array	Lists the forwarding rules of the forwarding policy. For details, see **Table 10-144**.
position	Integer	Specifies the forwarding priority. The value ranges from **1** to **100**. The default value is **100**. This parameter is reserved.
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the forwarding policy.

Table 10-159 rules parameter description

Parameter	Type	Description
id	String	Lists the IDs of the forwarding rules in the forwarding policy.

Example Request

- Example request: Updating a forwarding policy

```
PUT https://{Endpoint}/v2.0/lbaas/l7policies/5ae0e1e7-5f0f-47a1-b39f-5d4c428a1586

{
    "l7policy": {
        "name": "test"
    }
}
```

Example Response

- Example response

```
{
    "l7policy": {
        "redirect_pool_id": "431a03eb-81bb-408e-ae37-7ce19023692b",
        "redirect_listener_id": null,
        "description": "",
        "admin_state_up": true,
        "rules": [
            {
                "id": "67d8a8fa-b0dd-4bd4-a85b-671db19b2ef3"
            },
            {
                "id": "f02b3bca-69d2-4335-a3fa-a8054e996213"
            }
        ],

        "tenant_id": "a31d2bdcf7604c0faaddb058e1e08819",
        "project_id": "a31d2bdcf7604c0faaddb058e1e08819",
        "listener_id": "26058b64-6185-4e06-874e-4bd68b7633d0",
        "redirect_url": null,
        "action": "REDIRECT_TO_POOL",
        "provisioning_status": "ACTIVE",
        "position": 2,
        "id": "5ae0e1e7-5f0f-47a1-b39f-5d4c428a1586",
        "name": "test"
    }
}
```

Status Code

For details, see **Status Codes**.

10.1.6.5 Deleting a Forwarding Policy

Function

This API is used to delete a specific forwarding policy.

URI

DELETE /v2.0/lbaas/l7policies/{l7policy_id}

Table 10-160 Parameter description

Parameter	Mandatory	Type	Description
l7policy_id	Yes	Object	Specifies the forwarding policy ID.

Request

None

Response

None

Example Request

- Example request: Deleting a forwarding policy
  DELETE https://{Endpoint}/v2.0/lbaas/l7policies/5ae0e1e7-5f0f-47a1-b39f-5d4c428a1586

Example Response

- Example response
  None

Status Code

For details, see **Status Codes**.

10.1.7 Forwarding Rule

10.1.7.1 Adding a Forwarding Rule

Function

This API is used to add a forwarding rule. After you add a forwarding rule, the load balancer matches the domain name and path in the request and distributes the traffic to the backend server group specified by **redirect_pool_id** of the associated forwarding policy.

Constraints

The match type of forwarding rules in a forwarding policy must be unique.

URI

POST /v2.0/lbaas/l7policies/{l7policy_id}/rules

Table 10-161 Parameter description

Parameter	Mandatory	Type	Description
l7policy_id	Yes	String	Specifies the forwarding policy ID.

Request

Table 10-162 Parameter description

Parameter	Mandatory	Type	Description
rule	Yes	Object	Specifies the forwarding rule. For details, see **Table 10-163**.

Table 10-163 rule parameter description

Parameter	Mandatory	Type	Description
tenant_id	No	String	Specifies the ID of the project where the forwarding rule is used. The value must be the same as the value of **project_id** in the token. The value contains a maximum of 255 characters.
project_id	No	String	Specifies the ID of the project to which the forwarding rule belongs. This parameter has the same meaning as **tenant_id**. The value must be the same as the value of **project_id** in the token.
admin_state_up	No	Boolean	Specifies the administrative status of the forwarding rule. This parameter is reserved, and the default value is **true**.

Parameter	Mandatory	Type	Description
type	Yes	String	Specifies the match type of a forwarding rule. The value can be one of the following: • **HOST_NAME**: matches the domain name in the request. • **PATH**: matches the path in the request. The match type of forwarding rules in a forwarding policy must be unique.
compare_type	Yes	String	Specifies the match mode. The options are as follows: When **type** is set to **HOST_NAME**, the value of this parameter can only be the following: • **EQUAL_TO**: indicates exact match. When **type** is set to **PATH**, the value of this parameter can be one of the following: • **REGEX**: indicates regular expression match. • **STARTS_WITH**: indicates prefix match. • **EQUAL_TO**: indicates exact match.
invert	No	Boolean	Specifies whether reverse matching is supported. The value can be **true** or **false**. The default value is **false**. This parameter is reserved.
key	No	String	Specifies the key of the match content. The default value is **null**. This parameter is reserved. The value contains a maximum of 255 characters.

Parameter	Mandatory	Type	Description
value	Yes	String	Specifies the value of the match content. The value cannot contain spaces. The value contains a maximum of 128 characters. • When **type** is set to **HOST_NAME**, the value can contain a maximum of 100 characters that contain only letters, digits, hyphens (-), and periods (.), and must start with a letter or digit. • When **type** is set to **PATH**, the value can contain a maximum of 128 characters. When **compare_type** is set to **STARTS_WITH** or **EQUAL_TO**, the value must start with a slash (/) and can contain only letters, digits, and special characters _~';@^-%#&$.*+?,=!:| \/()[]{}

Response

Table 10-164 Response parameters

Parameter	Type	Description
rule	Object	Specifies the forwarding rule. For details, see **Table 10-165**.

Table 10-165 rule parameter description

Parameter	Type	Description
id	String	Specifies the forwarding rule ID.
tenant_id	String	Specifies the ID of the project where the forwarding rule is used. The value contains a maximum of 255 characters.
project_id	String	Specifies the ID of the project to which the forwarding rule belongs. This parameter has the same meaning as **tenant_id**.

Parameter	Type	Description
admin_state_up	Boolean	Specifies the administrative status of the forwarding rule. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
type	String	Specifies the match type of a forwarding rule. The value can be one of the following: • **HOST_NAME**: matches the domain name in the request. • **PATH**: matches the path in the request.
compare_type	String	Specifies the match mode. The options are as follows: When **type** is set to **HOST_NAME**, the value of this parameter can only be the following: • **EQUAL_TO**: indicates exact match. When **type** is set to **PATH**, the value of this parameter can be one of the following: • **REGEX**: indicates regular expression match. • **STARTS_WITH**: indicates prefix match. • **EQUAL_TO**: indicates exact match.
invert	Boolean	Specifies whether reverse matching is supported. The value can be **true** or **false**. The default value is **false**. This parameter is reserved.
key	String	Specifies the key of the match content. The default value is **null**. This parameter is reserved. The value contains a maximum of 255 characters.

Parameter	Type	Description
value	String	Specifies the value of the match content. The value contains a maximum of 128 characters. • When **type** is set to **HOST_NAME**, the value can contain a maximum of 100 characters that contain only letters, digits, hyphens (-), and periods (.), and must start with a letter or digit. • When **type** is set to **PATH**, the value can contain a maximum of 128 characters. When **compare_type** is set to **STARTS_WITH** or **EQUAL_TO**, the value must start with a slash (/) and can contain only letters, digits, and special characters _~';@^-%#&$.*+?,=!:| \/()[]{}
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the forwarding rule.

Example Request

- Example request: Adding a forwarding rule

```
POST https://{Endpoint}/v2.0/lbaas/l7policies/5ae0e1e7-5f0f-47a1-b39f-5d4c428a1586/rules

{
    "rule": {
        "compare_type": "EQUAL_TO",
        "type": "PATH",
        "value": "/bbb.html"
    }
}
```

Example Response

- Example response

```
{
    "rule": {
        "compare_type": "EQUAL_TO",
        "admin_state_up": true,
        "provisioning_status": "ACTIVE",
        "tenant_id": "a31d2bdcf7604c0faaddb058e1e08819",
        "project_id": "a31d2bdcf7604c0faaddb058e1e08819",
        "invert": false,
        "value": "/bbb.html",
        "key": null,
        "type": "PATH",
        "id": "c6f457b8-bf6f-45d7-be5c-a3226945b7b1"
    }
}
```

Status Code

For details, see **Status Codes**.

10.1.7.2 Querying Forwarding Rules

Function

This API is used to query forwarding rules. Filter query and pagination query are supported. Unless otherwise specified, exact match is applied.

Constraints

Parameters **marker**, **limit**, and **page_reverse** are used for pagination query. Parameters **marker** and **page_reverse** take effect only when they are used together with parameter **limit**.

URI

GET /v2.0/lbaas/l7policies/{l7policy_id}/rules

Table 10-166 Parameter description

Parameter	Mandatory	Type	Description
l7policy_id	Yes	String	Specifies the forwarding policy ID.

Request

Table 10-167 Parameter description

Parameter	Mandatory	Type	Description
marker	No	String	Specifies the ID of the forwarding rule from which pagination query starts, that is, the ID of the last forwarding rule on the previous page. This parameter must be used together with **limit**.
limit	No	Integer	Specifies the number of forwarding rules on each page. If this parameter is not set, all forwarding rules are queried by default.

Parameter	Mandatory	Type	Description
page_reverse	No	Boolean	Specifies the page direction. The value can be **true** or **false**, and the default value is **false**. The last page in the list requested with **page_reverse** set to **false** will not contain the "next" link, and the last page in the list requested with **page_reverse** set to **true** will not contain the "previous" link. This parameter must be used together with **limit**.
id	No	String	Specifies the forwarding rule ID.
tenant_id	No	String	Specifies the ID of the project where the forwarding rule is used. The value contains a maximum of 255 characters.
project_id	No	String	Specifies the ID of the project to which the forwarding rule belongs. This parameter has the same meaning as **tenant_id**.
admin_state_up	No	Boolean	Specifies the administrative status of the forwarding rule. This parameter is reserved, and the default value is **true**.
type	No	String	Specifies the match type of a forwarding rule. The value can be one of the following: • **HOST_NAME**: matches the domain name in the request. • **PATH**: matches the path in the request. The match type of forwarding rules in a forwarding policy must be unique.

Parameter	Mandatory	Type	Description
compare_type	No	String	Specifies the match mode. The options are as follows: When **type** is set to **HOST_NAME**, the value of this parameter can only be the following: • **EQUAL_TO**: indicates exact match. When **type** is set to **PATH**, the value of this parameter can be one of the following: • **REGEX**: indicates regular expression match. • **STARTS_WITH**: indicates prefix match. • **EQUAL_TO**: indicates exact match.
invert	No	Boolean	Specifies whether reverse matching is supported. The value can be **true** or **false**. The default value is **false**. This parameter is reserved.
key	No	String	Specifies the key of the match content. The default value is **null**. This parameter is reserved. The value contains a maximum of 255 characters.
value	No	String	Specifies the value of the match content. The value contains a maximum of 128 characters. • When **type** is set to **HOST_NAME**, the value can contain a maximum of 100 characters that contain only letters, digits, hyphens (-), and periods (.), and must start with a letter or digit. • When **type** is set to **PATH**, the value can contain a maximum of 128 characters. When **compare_type** is set to **STARTS_WITH** or **EQUAL_TO**, the value must start with a slash (/) and can contain only letters, digits, and special characters _~';@^-%#&$.*+?,=!:| \/()[]{}

Parameter	Mandatory	Type	Description
provisioning_status	No	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the forwarding rule.

Response

Table 10-168 Response parameters

Parameter	Type	Description
rules	Array	Lists the forwarding rules. For details, see **Table 10-169**.
rules_links	Array	Provides links to the previous or next page during pagination query, respectively. This parameter exists only in the response body of pagination query. For details, see **Table 10-170**.

Table 10-169 rules parameter description

Parameter	Type	Description
id	String	Specifies the forwarding rule ID.
tenant_id	String	Specifies the ID of the project where the forwarding rule is used. The value contains a maximum of 255 characters.
project_id	String	Specifies the ID of the project to which the forwarding rule belongs. This parameter has the same meaning as **tenant_id**.
admin_state_up	Boolean	Specifies the administrative status of the forwarding rule. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled

Parameter	Type	Description
type	String	Specifies the match type of a forwarding rule. The value can be one of the following: • **HOST_NAME**: matches the domain name in the request. • **PATH**: matches the path in the request.
compare_type	String	Specifies the match mode. The options are as follows: When **type** is set to **HOST_NAME**, the value of this parameter can only be the following: • **EQUAL_TO**: indicates exact match. When **type** is set to **PATH**, the value of this parameter can be one of the following: • **REGEX**: indicates regular expression match. • **STARTS_WITH**: indicates prefix match. • **EQUAL_TO**: indicates exact match.
invert	Boolean	Specifies whether reverse matching is supported. The value can be **true** or **false**. The default value is **false**. This parameter is reserved.
key	String	Specifies the key of the match content. The default value is **null**. This parameter is reserved. The value contains a maximum of 255 characters.
value	String	Specifies the value of the match content. The value contains a maximum of 128 characters. • When **type** is set to **HOST_NAME**, the value can contain a maximum of 100 characters that contain only letters, digits, hyphens (-), and periods (.), and must start with a letter or digit. • When **type** is set to **PATH**, the value can contain a maximum of 128 characters. When **compare_type** is set to **STARTS_WITH** or **EQUAL_TO**, the value must start with a slash (/) and can contain only letters, digits, and special characters _~';@^-%#&$.*+?,=!:| \/()[]{}

Parameter	Type	Description
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the forwarding rule.

Table 10-170 rules_links parameter description

Parameter	Type	Description
href	String	Provides links to the previous or next page during pagination query, respectively.
rel	String	Specifies the prompt of the previous or next page. The value can be **next** or **previous**. The value **next** indicates the href containing the URL of the next page, and **previous** indicates the href containing the URL of the previous page.

Example Request

- Example request: Querying all forwarding rules of a specific forwarding policy
  ```
  GET https://{Endpoint}/v2.0/lbaas/l7policies/5ae0e1e7-5f0f-47a1-b39f-5d4c428a1586/rules
  ```

Example Response

- Example response
  ```
  {
    "rules": [
      {
          "compare_type": "EQUAL_TO",
          "provisioning_status": "ACTIVE",
          "admin_state_up": true,
          "tenant_id": "a31d2bdcf7604c0faaddb058e1e08819",
          "project_id": "a31d2bdcf7604c0faaddb058e1e08819",
          "invert": false,
          "value": "www.test.com",
          "key": null,
          "type": "HOST_NAME",
          "id": "67d8a8fa-b0dd-4bd4-a85b-671db19b2ef3"
      },
      {
          "compare_type": "EQUAL_TO",
          "provisioning_status": "ACTIVE",
          "admin_state_up": true,
          "tenant_id": "a31d2bdcf7604c0faaddb058e1e08819",
          "project_id": "a31d2bdcf7604c0faaddb058e1e08819",
          "invert": false,
          "value": "/aaa.html",
          "key": null,
          "type": "PATH",
          "id": "f02b3bca-69d2-4335-a3fa-a8054e996213"
      }
    ]
    "rules_links": [
  ```



```
        {
        "href": "https://{Endpoint}/v2.0/lbaas/l7policies/061f461c-c7cf-47ab-9583-09be5076cd09/rules?
marker=167c1a31-bc12-4c3d-9ad1-c9bf450df4ce&page_reverse=True",
        "rel": "previous"
        }
    ]
}
```

Status Code

For details, see **Status Codes**.

10.1.7.3 Querying Details of a Forwarding Rule

Function

This API is used to query details about a forwarding rule by ID.

URI

GET /v2.0/lbaas/l7policies/{l7policy_id}/rules/{l7rule_id}

Table 10-171 Parameter description

Parameter	Mandatory	Type	Description
l7policy_id	Yes	String	Specifies the forwarding policy ID.
l7rule_id	Yes	String	Specifies the forwarding rule ID.

Request

None

Response

Table 10-172 Response parameters

Parameter	Type	Description
rule	Object	Specifies the forwarding rule. For details, see **Table 10-173**.

Table 10-173 rule parameter description

Parameter	Type	Description
id	String	Specifies the forwarding rule ID.

Parameter	Type	Description
tenant_id	String	Specifies the ID of the project where the forwarding rule is used. The value contains a maximum of 255 characters.
project_id	String	Specifies the ID of the project to which the forwarding rule belongs. This parameter has the same meaning as **tenant_id**.
admin_state_up	Boolean	Specifies the administrative status of the forwarding rule. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
type	String	Specifies the match type of a forwarding rule. The value can be one of the following: • **HOST_NAME**: matches the domain name in the request. • **PATH**: matches the path in the request.
compare_type	String	Specifies the match mode. The options are as follows: When **type** is set to **HOST_NAME**, the value of this parameter can only be the following: • **EQUAL_TO**: indicates exact match. When **type** is set to **PATH**, the value of this parameter can be one of the following: • **REGEX**: indicates regular expression match. • **STARTS_WITH**: indicates prefix match. • **EQUAL_TO**: indicates exact match.
invert	Boolean	Specifies whether reverse matching is supported. The value can be **true** or **false**. The default value is **false**. This parameter is reserved.
key	String	Specifies the key of the match content. The default value is **null**. This parameter is reserved. The value contains a maximum of 255 characters.

Parameter	Type	Description
value	String	Specifies the value of the match content. The value contains a maximum of 128 characters. • When **type** is set to **HOST_NAME**, the value can contain a maximum of 100 characters that contain only letters, digits, hyphens (-), and periods (.), and must start with a letter or digit. • When **type** is set to **PATH**, the value can contain a maximum of 128 characters. When **compare_type** is set to **STARTS_WITH** or **EQUAL_TO**, the value must start with a slash (/) and can contain only letters, digits, and special characters _~';@^-%#&$.*+?,=!:| \/()[]{}
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the forwarding rule.

Example Request

- Example request: Querying details of a forwarding rule

```
GET https://{Endpoint}/v2.0/lbaas/l7policies/5ae0e1e7-5f0f-47a1-b39f-5d4c428a1586/rules/67d8a8fa-b0dd-4bd4-a85b-671db19b2ef3
```

Example Response

- Example response

```
{
    "rule": {
        "compare_type": "EQUAL_TO",
        "provisioning_status": "ACTIVE",
        "admin_state_up": true,
        "tenant_id": "a31d2bdcf7604c0faaddb058e1e08819",
        "project_id": "a31d2bdcf7604c0faaddb058e1e08819",
        "invert": false,
        "value": "/index.html",
        "key": null,
        "type": "PATH",
        "id": "67d8a8fa-b0dd-4bd4-a85b-671db19b2ef3"
    }
}
```

Status Code

For details, see **Status Codes**.

10.1.7.4 Updating a Forwarding Rule

Function

This API is used to update a forwarding rule. You can change the mode that how traffic is distributed by updating the forwarding rule.

URI

PUT /v2.0/lbaas/l7policies/{l7policy_id}/rules/{l7rule_id}

Table 10-174 Parameter description

Parameter	Mandatory	Type	Description
l7policy_id	Yes	String	Specifies the forwarding policy ID.
l7rule_id	Yes	String	Specifies the forwarding rule ID.

Request

Table 10-175 Parameter description

Parameter	Mandatory	Type	Description
rule	Yes	Object	Specifies the forwarding rule. For details, see **Table 10-176**.

Table 10-176 rule parameter description

Parameter	Mandatory	Type	Description
compare_type	No	String	Specifies the match mode. The options are as follows: When **type** is set to **HOST_NAME**, the value of this parameter can only be the following: • **EQUAL_TO**: indicates exact match. When **type** is set to **PATH**, the value of this parameter can be one of the following: • **REGEX**: indicates regular expression match. • **STARTS_WITH**: indicates prefix match. • **EQUAL_TO**: indicates exact match.

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Specifies the administrative status of the forwarding rule. This parameter is reserved, and the default value is **true**.
invert	No	Boolean	Specifies whether reverse matching is supported. The value can be **true** or **false**. The default value is **false**. This parameter is reserved.
key	No	String	Specifies the key of the match content. The default value is **null**. This parameter is reserved. The value contains a maximum of 255 characters.
value	No	String	Specifies the value of the match content. The value cannot contain spaces. The value contains a maximum of 128 characters. • When **type** is set to **HOST_NAME**, the value can contain a maximum of 100 characters that contain only letters, digits, hyphens (-), and periods (.), and must start with a letter or digit. • When **type** is set to **PATH**, the value can contain a maximum of 128 characters. When **compare_type** is set to **STARTS_WITH** or **EQUAL_TO**, the value must start with a slash (/) and can contain only letters, digits, and special characters _~';@^-%#&$.* +?,=!:| \/()[]{}

Response

Table 10-177 Response parameters

Parameter	Type	Description
rule	Object	Specifies the forwarding rule. For details, see **Table 10-178**.

Table 10-178 rule parameter description

Parameter	Type	Description
id	String	Specifies the forwarding rule ID.
tenant_id	String	Specifies the ID of the project where the forwarding rule is used. The value contains a maximum of 255 characters.
project_id	String	Specifies the ID of the project to which the forwarding rule belongs. This parameter has the same meaning as **tenant_id**.
admin_state_up	Boolean	Specifies the administrative status of the forwarding rule. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
type	String	Specifies the match type of a forwarding rule. The value can be one of the following: • **HOST_NAME**: matches the domain name in the request. • **PATH**: matches the path in the request.
compare_type	String	Specifies the match mode. The options are as follows: When **type** is set to **HOST_NAME**, the value of this parameter can only be the following: • **EQUAL_TO**: indicates exact match. When **type** is set to **PATH**, the value of this parameter can be one of the following: • **REGEX**: indicates regular expression match. • **STARTS_WITH**: indicates prefix match. • **EQUAL_TO**: indicates exact match.
invert	Boolean	Specifies whether reverse matching is supported. The value can be **true** or **false**. The default value is **false**. This parameter is reserved.
key	String	Specifies the key of the match content. The default value is **null**. This parameter is reserved. The value contains a maximum of 255 characters.

Parameter	Type	Description
value	String	Specifies the value of the match content. The value contains a maximum of 128 characters. • When **type** is set to **HOST_NAME**, the value can contain a maximum of 100 characters that contain only letters, digits, hyphens (-), and periods (.), and must start with a letter or digit. • When **type** is set to **PATH**, the value can contain a maximum of 128 characters. When **compare_type** is set to **STARTS_WITH** or **EQUAL_TO**, the value must start with a slash (/) and can contain only letters, digits, and special characters _~';@^-%#&$.*+?,=!:| \/()[]{}
provisioning_status	String	This parameter is reserved, and its value can only be **ACTIVE**. It specifies the provisioning status of the forwarding rule.

Example Request

- Example request: Updating a forwarding rule

```
PUT https://{Endpoint}/v2.0/lbaas/l7policies/5ae0e1e7-5f0f-47a1-b39f-5d4c428a1586/rules/c6f457b8-bf6f-45d7-be5c-a3226945b7b1

{
    "rule": {
        "compare_type": "STARTS_WITH",
        "value": "/ccc.html"
    }
}
```

Example Response

- Example response

```
{
    "rule": {
        "compare_type": "STARTS_WITH",
        "provisioning_status": "ACTIVE",
        "admin_state_up": true,
        "tenant_id": "a31d2bdcf7604c0faaddb058e1e08819",
        "project_id": "a31d2bdcf7604c0faaddb058e1e08819",
        "invert": false,
        "value": "/ccc.html",
        "key": null,
        "type": "PATH",
        "id": "c6f457b8-bf6f-45d7-be5c-a3226945b7b1"
    }
}
```

Status Code

For details, see **Status Codes**.

10.1.7.5 Deleting a Forwarding Rule

Function

This API is used to delete a specific forwarding rule.

URI

DELETE /v2.0/lbaas/l7policies/{l7policy_id}/rules/{l7rule_id}

Table 10-179 Parameter description

Parameter	Mandatory	Type	Description
l7policy_id	Yes	String	Specifies the forwarding policy ID.
l7rule_id	Yes	String	Specifies the forwarding rule ID.

Request

None

Response

None

Example Request

- Example request: Deleting a forwarding rule
  ```
  DELETE https://{Endpoint}/v2.0/lbaas/l7policies/5ae0e1e7-5f0f-47a1-b39f-5d4c428a1586/rules/c6f457b8-bf6f-45d7-be5c-a3226945b7b1
  ```

Example Response

- Example response

  None

Status Code

For details, see **Status Codes**.

10.1.8 Whitelist

10.1.8.1 Adding a Whitelist

Function

This API is used to add a whitelist to control access to a specific listener. After a whitelist is added, only IP addresses in the whitelist can access the listener.

URI

POST /v2.0/lbaas/whitelists

Request

Table 10-180 Parameter description

Parameter	Mandatory	Type	Description
whitelist	Yes	Object	Specifies the whitelist. For details, see **Table 10-181**.

Table 10-181 whitelist parameter description

Parameter	Mandatory	Type	Description
tenant_id	No	String	Specifies the ID of the project where the whitelist is used. The value must be the same as the value of **project_id** in the token. The value contains a maximum of 255 characters.
listener_id	Yes	String	Specifies the listener ID. Only one whitelist can be created for a listener.
enable_whitelist	No	Boolean	Specifies whether to enable access control. **true**: Access control is enabled. **false**: Access control is disabled. The default value is **true**.
whitelist	No	String	Specifies the IP addresses in the whitelist. Use commas (,) to separate multiple IP addresses. You can specify an IP address, for example, 192.168.11.1. You can also specify an IP address range, for example, 192.168.0.1/24. The default value is an empty string, that is, **""**.

Response

Table 10-182 Response parameters

Parameter	Type	Description
whitelist	Object	Specifies the whitelist. For details, see **Table 10-183**.

Table 10-183 whitelist parameter description

Parameter	Type	Description
id	String	Specifies the whitelist ID.
tenant_id	String	Specifies the ID of the project where the whitelist is used. The value contains a maximum of 255 characters.
listener_id	String	Specifies the ID of the listener to which the whitelist is added.
enable_whitelist	Boolean	Specifies whether to enable access control. **true**: Access control is enabled. **false**: Access control is disabled.
whitelist	String	Specifies the IP addresses in the whitelist.

Example Request

- Example request: Adding a whitelist

```
POST https://{Endpoint}/v2.0/lbaas/whitelists

{
    "whitelist": {
        "listener_id": "eabfefa3fd1740a88a47ad98e132d238",
        "enable_whitelist": true,
        "whitelist": "192.168.11.1,192.168.0.1/24,192.168.201.18/8,100.164.0.1/24"
    }
}
```

Example Response

- Example response

```
{
    "whitelist": {
        "id": "eabfefa3fd1740a88a47ad98e132d238",
        "listener_id": "eabfefa3fd1740a88a47ad98e132d238",
        "tenant_id": "eabfefa3fd1740a88a47ad98e132d238",
        "enable_whitelist": true,
        "whitelist": "192.168.11.1,192.168.0.1/24,192.168.201.18/8,100.164.0.1/24"
```



```
  }
}
```

Status Code

For details, see **Status Codes**.

10.1.8.2 Querying Whitelists

Function

This API is used to query the whitelists. Filter query and pagination query are supported. Unless otherwise specified, exact match is applied.

Constraints

Parameters **marker**, **limit**, and **page_reverse** are used for pagination query. Parameters **marker** and **page_reverse** take effect only when they are used together with parameter **limit**.

URI

GET /v2.0/lbaas/whitelists

Request

Table 10-184 Parameter description

Parameter	Mandatory	Type	Description
marker	No	String	Specifies the ID of the whitelist from which pagination query starts, that is, the ID of the last whitelist on the previous page. This parameter must be used together with **limit**.
limit	No	Integer	Specifies the number of whitelists on each page. If this parameter is not set, all whitelists are queried by default.

Parameter	Mandatory	Type	Description
page_reverse	No	Boolean	Specifies the page direction. The value can be **true** or **false**, and the default value is **false**. The last page in the list requested with **page_reverse** set to **false** will not contain the "next" link, and the last page in the list requested with **page_reverse** set to **true** will not contain the "previous" link. This parameter must be used together with **limit**.
id	No	String	Specifies the whitelist ID.
tenant_id	No	String	Specifies the ID of the project where the whitelist is used. The value contains a maximum of 255 characters.
listener_id	No	String	Specifies the ID of the listener to which the whitelist is added.
enable_whitelist	No	Boolean	Specifies whether to enable access control. **true**: Access control is enabled. **false**: Access control is disabled.
whitelist	No	String	Specifies the IP addresses in the whitelist.

Response

Table 10-185 Response parameters

Parameter	Type	Description
whitelists	Array	Lists the whitelists. For details, see **Table 10-186**.
whitelists_links	Array	Provides links to the previous or next page during pagination query, respectively. This parameter exists only in the response body of pagination query. For details, see **Table 10-187**.

Table 10-186 whitelist parameter description

Parameter	Type	Description
id	String	Specifies the whitelist ID.
tenant_id	String	Specifies the ID of the project where the whitelist is used. The value contains a maximum of 255 characters.
listener_id	String	Specifies the ID of the listener to which the whitelist is added.
enable_whitelist	Bool	Specifies whether to enable access control. **true**: Access control is enabled. **false**: Access control is disabled.
whitelist	String	Specifies the IP addresses in the whitelist.

Table 10-187 whitelists_links parameter description

Parameter	Type	Description
href	String	Provides links to the previous or next page during pagination query, respectively.
rel	String	Specifies the prompt of the previous or next page. The value can be **next** or **previous**. The value **next** indicates the href containing the URL of the next page, and **previous** indicates the href containing the URL of the previous page.

Example Request

- Example request 1: Querying all whitelists
  ```
  GET https://{Endpoint}/v2.0/lbaas/whitelists
  ```
- Example request 2: Querying the whitelists added to listener eabfefa3fd1740a88a47ad98e132d230
  ```
  GET https://{Endpoint}/v2.0/lbaas/whitelists?listener_id=eabfefa3fd1740a88a47ad98e132d230
  ```

Example Response

- Example response 1


```
{
    "whitelists": [
        {
            "id": "eabfefa3fd1740a88a47ad98e132d238",
            "listener_id": "eabfefa3fd1740a88a47ad98e132d238",
            "tenant_id": "eabfefa3fd1740a88a47ad98e132d238",
            "enable_whitelist": true,
            "whitelist": "192.168.11.1,192.168.0.1/24,192.168.201.18/8,100.164.0.1/24"
        },
        {
            "id": "eabfefa3fd1740a88a47ad98e132d326",
            "listener_id": "eabfefa3fd1740a88a47ad98e132d327",
            "tenant_id": "eabfefa3fd1740a88a47ad98e132d436",
            "enable_whitelist": true,
            "whitelist": "192.168.12.1,192.168.1.1/24,192.168.203.18/8,100.164.5.1/24"
        }
    ]
}
```

- Example response 2

```
{
    "whitelists": [
        {
            "id": "eabfefa3fd1740a88a47ad98e132d238",
            "listener_id": "eabfefa3fd1740a88a47ad98e132d230",
            "tenant_id": "eabfefa3fd1740a88a47ad98e132d239",
            "enable_whitelist": true,
            "whitelist": "192.168.11.1,192.168.0.1/24,192.168.201.18/8,100.164.0.1/24"
        },
        {
            "id": "eabfefa3fd1740a88a47ad98e132d326",
            "listener_id": "eabfefa3fd1740a88a47ad98e132d327",
            "tenant_id": "eabfefa3fd1740a88a47ad98e132d439",
            "enable_whitelist": true,
            "whitelist": "192.168.12.1,192.168.1.1/24,192.168.203.18/8,100.164.5.1/24"
        }
    ]
}
```

Status Code

For details, see **Status Codes**.

10.1.8.3 Querying Details of a Whitelist

Function

This API is used to query details about a whitelist using its ID.

URI

GET /v2.0/lbaas/whitelists/{whitelist_id}

Table 10-188 Parameter description

Parameter	Mandatory	Type	Description
whitelist_id	Yes	String	Specifies the whitelist ID.

Request

None

Response

Table 10-189 Response parameters

Parameter	Type	Description
whitelist	Object	Specifies the whitelist. For details, see **Table 10-190**.

Table 10-190 whitelist parameter description

Parameter	Type	Description
id	String	Specifies the whitelist ID.
tenant_id	String	Specifies the ID of the project where the forwarding rule is used. The value contains a maximum of 255 characters.
listener_id	String	Specifies the ID of the listener to which the whitelist is added.
enable_whitelist	Boolean	Specifies whether to enable access control. **true**: Access control is enabled. **false**: Access control is disabled.
whitelist	String	Specifies the IP addresses in the whitelist.

Example Request

- Example request: Querying details of a whitelist
  ```
  GET https://{Endpoint}/v2.0/lbaas/whitelists/09e64049-2ab0-4763-a8c5-f4207875dc3e
  ```

Example Response

- Example response
  ```
  {
     "whitelist": {
        "id": "eabfefa3fd1740a88a47ad98e132d238",
        "listener_id": "eabfefa3fd1740a88a47ad98e132d238",
        "tenant_id": "eabfefa3fd1740a88a47ad98e132d238",
        "enable_whitelist": true,
        "whitelist": "192.168.11.1,192.168.0.1/24,192.168.201.18/8,100.164.0.1/24"
     }
  }
  ```


Status Code

For details, see **Status Codes**.

10.1.8.4 Updating a Whitelist

Function

This API is used to update a whitelist. You can enable or disable the whitelist function or change IP addresses in the whitelist. If you change IP addresses in the whitelist, it will be deleted, and a new one is generated.

URI

PUT /v2.0/lbaas/whitelists/{whitelist_id}

Table 10-191 Parameter description

Parameter	Mandatory	Type	Description
whitelist_id	Yes	String	Specifies the whitelist ID.

Request

Table 10-192 Parameter description

Parameter	Mandatory	Type	Description
whitelist	Yes	Object	Specifies the whitelist. For details, see **Table 10-193**.

Table 10-193 whitelist parameter description

Parameter	Mandatory	Type	Description
enable_whitelist	No	Boolean	Specifies whether to enable access control. **true**: Access control is enabled. **false**: Access control is disabled. The default value is **true**.

Parameter	Mandatory	Type	Description
whitelist	No	String	Specifies the IP addresses in the whitelist. Use commas (,) to separate multiple IP addresses. You can specify an IP address, for example, 192.168.11.1. You can also specify an IP address range, for example, 192.168.0.1/24. The default value is an empty string, that is, "".

Response

Table 10-194 Parameter description

Parameter	Type	Description
whitelist	Object	Specifies the whitelist. For details, see **Table 10-195**.

Table 10-195 whitelist parameter description

Parameter	Type	Description
id	String	Specifies the whitelist ID.
tenant_id	String	Specifies the ID of the project where the whitelist is used. The value contains a maximum of 255 characters.
listener_id	String	Specifies the ID of the listener to which the whitelist is added.
enable_whitelist	Boolean	Specifies whether to enable access control. **true**: Access control is enabled. **false**: Access control is disabled.
whitelist	String	Specifies the IP addresses in the whitelist.

Example Request

- Example request: Updating a whitelist

```
PUT https://{Endpoint}/v2.0/lbaas/whitelists/dcaf46f1-037c-4f63-a31f-e0c4c18032c7

{
```



```
    "whitelist": {
        "enable_whitelist": true,
        "whitelist": "192.168.11.1,192.168.0.1/24,192.168.201.18/8,100.164.0.1/24"
    }
}
```

Example Response

- Example response

```
{
    "whitelist": {
        "id": "eabfefa3fd1740a88a47ad98e132d238",
        "listener_id": "eabfefa3fd1740a88a47ad98e132d238",
        "tenant_id": "eabfefa3fd1740a88a47ad98e132d238",
        "enable_whitelist": true,
        "whitelist": "192.168.11.1,192.168.0.1/24,192.168.201.18/8,100.164.0.1/24"
    }
}
```

Status Code

For details, see **Status Codes**.

10.1.8.5 Deleting a Whitelist

Function

This API is used to delete a specific whitelist.

URI

DELETE /v2.0/lbaas/whitelists/{whitelist_id}

Table 10-196 Parameter description

Parameter	Mandatory	Type	Description
whitelist_id	Yes	String	Specifies the whitelist ID.

Request

None

Response

None

Example Request

- Example request: Deleting a whitelist

```
DELETE https://{Endpoint}/v2.0/lbaas/whitelists/35cb8516-1173-4035-8dae-0dae3453f37f
```

Example Response

- Example response 1

None

Status Code

For details, see **Status Codes**.

10.1.9 Certificate

10.1.9.1 Creating a Certificate

Function

This API is used to create a certificate. After a certificate is bound to a listener, the load balancer authenticates the client using this certificate, and backend servers can establish secure and reliable HTTP connections with the client.

URI

POST /v2.0/lbaas/certificates

Request

Table 10-197 Parameter description

Parameter	Mandatory	Type	Description
tenant_id	No	String	Specifies the ID of the project where the certificate is used. The value must be the same as the value of **project_id** in the token. The value contains a maximum of 255 characters.
admin_state_up	No	Boolean	Specifies the administrative status of the certificate. This parameter is reserved, and the default value is **true**.
name	No	String	Specifies the certificate name. The value contains a maximum of 255 characters.
description	No	String	Provides supplementary information about the certificate. The value contains a maximum of 255 characters.

Parameter	Mandatory	Type	Description
type	No	String	Specifies the certificate type. The default value is **server**. The value can be one of the following: ● **server**: indicates the server certificate. ● **client**: indicates the CA certificate.
domain	No	String	Specifies the domain name associated with the server certificate. A domain name can contain up to 100 characters. You can specify up to 30 domain names and separate them using commas (,). The value can be one of the following: ● A common domain name contains 0 to 100 characters and consists of several labels separated by periods (.). Each label can contain a maximum of 63 characters, including letters, digits, and hyphens (-), and must start and end with a letter or digit. Example: www.test.com ● In addition to the requirements for common domain names, a wildcard domain name can start with an asterisk (*). Example: *.test.com **NOTE** ● This parameter is valid only when **type** is set to **server**.
private_key	No	String	Specifies the private key of the server certificate. The value must be PEM encoded. ● This parameter will be ignored if **type** is set to **client**. A CA server can still be created and used normally. This parameter will be left blank even if you enter a private key that is not PEM encoded. ● This parameter is valid and mandatory only when **type** is set to **server**. If you enter an invalid private key, an error is returned.
certificate	Yes	String	Specifies the public key of the server certificate or CA certificate used to authenticate the client. The value of parameter **type** determines whether a public key or CA certificate is required. The public key is in PEM format.

Response

Table 10-198 Parameter description

Parameter	Type	Description
id	String	Specifies the certificate ID.
tenant_id	String	Specifies the ID of the project where the certificate is used. The value contains a maximum of 255 characters.
admin_state_up	Boolean	Specifies the administrative status of the certificate. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
name	String	Specifies the certificate name. The value contains a maximum of 255 characters.
description	String	Provides supplementary information about the certificate. The value contains a maximum of 255 characters.
type	String	Specifies the certificate type. The value can be one of the following: • **server**: indicates the server certificate. • **client**: indicates the CA certificate.

Parameter	Type	Description
domain	String	Specifies the domain name associated with the server certificate. A domain name can contain up to 100 characters. You can specify up to 30 domain names and separate them using commas (,). The value can be one of the following: ● A common domain name contains 0 to 100 characters and consists of several labels separated by periods (.). Each label can contain a maximum of 63 characters, including letters, digits, and hyphens (-), and must start and end with a letter or digit. Example: www.test.com ● In addition to the requirements for common domain names, a wildcard domain name can start with an asterisk (*). Example: *.test.com **NOTE** ● This parameter is valid only when **type** is set to **server**.
private_key	String	Specifies the private key of the server certificate in PEM format.
certificate	String	Specifies the public key of the server certificate or CA certificate used to authenticate the client. The value of parameter **type** determines whether a public key or CA certificate is required. Both types of certificates are in PEM format.
expire_time	String	Specifies the time when the certificate expired. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format.
create_time	String	Specifies the time when the certificate was created. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format.
update_time	String	Specifies the time when the certificate was updated. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format.

Example Request

- Example request: Creating a certificate
  ```
  POST https://{Endpoint}/v2.0/lbaas/certificates
  ```



```
{
    "name": "https_certificate",
    "description": "description for certificate",
    "type": "server",
    "domain": "www.elb.com",
    "private_key":
"-----BEGIN PRIVATE KEY-----
\nMIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDQVAbOLe5xNf4M
\n253Wn9vhdUzojetjv4J+B7kYwsMhRcgdcJ8KCnX1nfzTvI2ksXlTQ2o9BkpStnPe\ntB4s32ZiJRMlk
+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM
\nMD30gLh6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8Icq39buNpIgDOWzEP5AzqXt
\nCOFYn6RTH5SRug4hKNN7sT1eYMslHu7wtEBDKVgrLjOCe/W2f8rLT1zEsoAW2Chl\nZAPYUBkl/
0XuTWRg3CohPPcI+UtlRSfvLDeeQ460swjbwgS/RbJh3sIwlCRLU08k\nEo04Z9H/
AgMBAAECggEAEIeaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/Hl
\nfvCArftGgMaYWPSNCJRMXB7tPwpQu19esjz4Z/cR2Je4fTLPrffGUsHFgZjv5OQB
\nZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr
\nciu9YkInNEHu6uRJ5g/eGGX3KQynTvVIhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M\nEGpfYI6AdHIwFZcT/
RNAxhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7Ale\nkrguPtfV1vWklg
+bUFhgGaiAEYTpAUN9t2DVIiijgQKBgQDnYMMsaF0r557CM1CT
\nXUqgCZo8MKeV2jf2drlxRRwRl33SksQbzAQ/qrLdT7GP3sCGqvkxWY2FPdFYf8kx
\nGcCeZPcIeZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/fbwjpjP7dt
\nJ7n8EzkRUNE6aIMHOFEeych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr
\niWgTWHXPZxUQaYhpjXo6+lMI6DpExiDgBAkMzJGIvS7yQiYWU+wthAr9urbWYdGZ
\nlS6VjoTkF6r7VZoILXX0fbuXh6lm8K8IQRfBpJff56p9phMwaBpDNDrfpHB5utBU
\nxs40yIdp6wKBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zJf3bGSXU/jR4eB
\n1lVQhELGI9CbKSdzKM71GyEImix/T7FnJSHIWlho1qVo6AQyduNWnAQD15pr8KAd
\nXGXAZZ1FQcb3KYa+2fflERmazdOTwjYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak\n/
735uP20KKqhNehZpC2dJei7OiIgRhCS/dKASUXHSW4fptBnUxACYocdDxtY4Vha\nfI7FPMdvGl8ioYbvlHFh
+X0Xs9r1S8yeWnHoXMb6eXWmYKMJrAoveLa+2cFm1Agf
\n7nLhA4R4lqm9IpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAJkD4wHW54Pwd4Ctfk9o
\njHjWB7pQlUYpTZO9dm+4fpCMn9Okf43AE2yAOaAP94GdzdDJkxfciXKcsYr9IIuk
\nfaoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BUlGKMWXzuEd\n3fy
+1rCUwzOp9LSjtJYf4ege\n-----END PRIVATE KEY-----",
    "certificate":
"-----BEGIN CERTIFICATE-----
\nMIIC4TCCAcmgAwIBAgICEREwDQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXlD
\nb21wYW55IENBMB4XDTE4MDcwMjEzMjU0N1oXDTQ1MTExNzEzMjU0N1owFDESMBAG
\nA1UEAwwJbG9jYWxob3N0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA\n0FQGzi3ucTX
+DNud1p/
b4XVM6I3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5\nU0NqPQZKUrZz3rQeLN9mYiUTJZPutYlFDDb
B8CtlgV+eyU9yYJslWx/
Bm5kWNPh9\n7B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/W7jaS
\nIAzlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylYKy4zgnv1tn/K
\ny09cxLKAFtgoZWQD2FAZJf9F7k1kYNwqITz3CPlLZUUn7yw3nkOOtLMI28IEv0Wy
\nYd7CMJQkS1NPJBKNOGfR/wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29t
\nhwQKuUvJhwR/AAABMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCSqGSIb3DQEBCwUA
\nA4IBAQA8lMQJxaTey7EjXtRLSVlEAMftAQPG6jijNQuvIBQYUDauDT4W2XUZ5wAn
\njiOyQ83va672K1G9s8n6xlH+xwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDa
\nezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPRLYlzp1HMnI6hkjPk4PCZ
\nwKnha0dlScati9CCt3UzXSNJOSLalKdHErH08Iqd+1BchScxCfk0xNITn1HZZGmI\n
+vbmunok3A2lucI14rnsrcbkGYqxGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZ\niYsGDVN
+9QBd0eYUHce+77s96i3I\n-----END CERTIFICATE-----"
}
```


Example Response

- Example response


```
{
    "domain": "www.elb.com",
    "expire_time": "2045-11-17 13:25:47",
    "update_time": "2017-12-04 06:49:13",
    "create_time": "2017-12-04 06:49:13",
    "id": "3d8a7a02f87a40ed931b719edfe75451",
    "admin_state_up": true,
    "private_key": "-----BEGIN PRIVATE KEY-----
\nMIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDQVAbOLe5xNf4M
\n253Wn9vhdUzojetjv4J+B7kYwsMhRcgdcJ8KCnX1nfzTvI2ksXlTQ2o9BkpStnPe\ntB4s32ZiJRMlk
+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM
\nMD30gLh6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8Icq39buNpIgDOWzEP5AzqXt
```


\nCOFYn6RTH5SRug4hKNN7sT1eYMslHu7wtEBDKVgrLjOCe/W2f8rLT1zEsoAW2Chl\nZAPYUBkl/
0XuTWRg3CohPPcl+UtlRSfvLDeeQ460swjbwgS/RbJh3slwlCRLU08k\nEo04Z9H/
AgMBAAECggEAEIeaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/Hl
\nfvCArftGgMaYWPSNCJRMXB7tPwpQu19esjz4Z/cR2Je4fTLPrffGUsHFgZjv5OQB
\nZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr
\nciu9YkInNEHu6uRJ5g/eGGX3KQynTvVIhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M\nEGpfYI6AdHIwFZcT/
RNAxhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7Ale\nkrguPtfV1vWklg
+bUFhgGaiAEYTpAUN9t2DVIiijgQKBgQDnYMMsaF0r557CM1CT
\nXUqgCZo8MKeV2jf2drlxRRwRl33SksQbzAQ/qrLdT7GP3sCGqvkxWY2FPdFYf8kx
\nGcCeZPcIeZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/fbwjpjP7dt
\nJ7n8EzkRUNE6aIMHOFEeych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr
\niWgTWHXPZxUQaYhpjXo6+lMI6DpExiDgBAkMzJGIvS7yQiYWU+wthAr9urbWYdGZ
\nlS6VjoTkF6r7VZoILXX0fbuXh6lm8K8IQRfBpJff56p9phMwaBpDNDrfpHB5utBU
\nxs40yIdp6wKBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zJf3bGSXU/jR4eB
\n1lVQhELGI9CbKSdzKM71GyEImix/T7FnJSHIWlho1qVo6AQyduNWnAQD15pr8KAd
\nXGXAZZ1FQcb3KYa+2fflERmazdOTwjYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak\n/
735uP20KKqhNehZpC2dJei7OiIgRhCS/dKASUXHSW4fptBnUxACYocdDxtY4Vha\nfI7FPMdvGl8ioYbvlHFh
+X0Xs9r1S8yeWnHoXMb6eXWmYKMJrAoveLa+2cFm1Agf
\n7nLhA4R4lqm9IpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAJkD4wHW54Pwd4Ctfk9o
\njHjWB7pQlUYpTZO9dm+4fpCMn9Okf43AE2yAOaAP94GdzdDJkxfciXKcsYr9IIuk
\nfaoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BUlGKMWXzuEd\n3fy
+1rCUwzOp9LSjtJYf4ege\n-----END PRIVATE KEY-----",
    "tenant_id": "930600df07ac4f66964004041bd3deaf",
    "type": "server",
    "certificate": "-----BEGIN CERTIFICATE-----
\nMIIC4TCCAcmgAwIBAgICEREwDQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXlD
\nb21wYW55IENBMB4XDTE4MDcwMjEzMjU0N1oXDTQ1MTExNzEzMjU0N1owFDESMBAG
\nA1UEAwwJbG9jYWxob3N0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA\n0FQGzi3ucTX
+DNud1p/
b4XVM6I3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5\nU0NqPQZKUrZz3rQeLN9mYiUTJZPutYlFDDb
B8CtlgV+eyU9yYJslWx/
Bm5kWNPh9\n7B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/W7jaS
\nIAzlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylYKy4zgnv1tn/K
\ny09cxLKAFtgoZWQD2FAZJf9F7k1kYNwqITz3CPlLZUUn7yw3nkOOtLMI28IEv0Wy
\nYd7CMJQkS1NPJBKNOGfR/wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29t
\nhwQKuUvJhwR/AAABMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCSqGSIb3DQEBCwUA
\nA4IBAQA8lMQJxaTey7EjXtRLSVlEAMftAQPG6jijNQuvIBQYUDauDT4W2XUZ5wAn
\njiOyQ83va672K1G9s8n6xlH+xwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDa
\nezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPRLYlzp1HMnI6hkjPk4PCZ
\nwKnha0dlScati9CCt3UzXSNJOSLalKdHErH08Iqd+1BchScxCfk0xNITn1HZZGmI\n
+vbmunok3A2lucI14rnsrcbkGYqxGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZ\niYsGDVN
+9QBd0eYUHce+77s96i3l\n-----END CERTIFICATE-----",
    "name": "https_certificate",
    "description": "description for certificate"
}

Status Code

For details, see **Status Codes**.

10.1.9.2 Querying Certificates

Function

This API is used to query all the certificates. Filter query and pagination query are supported. Unless otherwise specified, exact match is applied.

Constraints

Parameters **marker**, **limit**, and **page_reverse** are used for pagination query. Parameters **marker** and **page_reverse** take effect only when they are used together with parameter **limit**.

URI

GET /v2.0/lbaas/certificates

Request

Table 10-199 Parameter description

Parameter	Mandatory	Type	Description
marker	No	String	Specifies the ID of the certificate from which pagination query starts, that is, the ID of the last certificate on the previous page. This parameter must be used together with **limit**.
limit	No	Integer	Specifies the number of certificates on each page. If this parameter is not set, all certificates are queried by default.
page_reverse	No	Boolean	Specifies the page direction. The value can be **true** or **false**, and the default value is **false**. The last page in the list requested with **page_reverse** set to **false** will not contain the "next" link, and the last page in the list requested with **page_reverse** set to **true** will not contain the "previous" link. This parameter must be used together with **limit**.
id	No	String	Specifies the certificate ID.
name	No	String	Specifies the certificate name. The value contains a maximum of 255 characters.
description	No	String	Provides supplementary information about the certificate. The value contains a maximum of 255 characters.

Parameter	Mandatory	Type	Description
type	No	String	Specifies the certificate type. The default value is **server**. The value can be one of the following: ● **server**: indicates the server certificate. ● **client**: indicates the CA certificate.
domain	No	String	Specifies the domain name associated with the server certificate. A domain name can contain up to 100 characters. You can specify up to 30 domain names and separate them using commas (,). The value can be one of the following: ● A common domain name contains 0 to 100 characters and consists of several labels separated by periods (.). Each label can contain a maximum of 63 characters, including letters, digits, and hyphens (-), and must start and end with a letter or digit. Example: www.test.com ● In addition to the requirements for common domain names, a wildcard domain name can start with an asterisk (*). Example: *.test.com **NOTE** ● This parameter is valid only when **type** is set to **server**.

Parameter	Mandatory	Type	Description
private_key	No	String	Specifies the private key of the server certificate. The value must be PEM encoded. • This parameter will be ignored if **type** is set to **client**. A CA server can still be created and used normally. This parameter will be left blank even if you enter a private key that is not PEM encoded. • This parameter is valid and mandatory only when **type** is set to **server**. If you enter an invalid private key, an error is returned.
certificate	No	String	Specifies the public key of the server certificate or CA certificate used to authenticate the client. The value of parameter **type** determines whether a public key or CA certificate is required. Both types of certificates are in PEM format.
create_time	No	String	Specifies the time when the certificate was created. The UTC time is in *YYYY-MM-DD HH:MM:SS* format.
update_time	No	String	Specifies the time when the certificate was updated. The UTC time is in *YYYY-MM-DD HH:MM:SS* format.

Response

Table 10-200 Parameter description

Parameter	Type	Description
certificates	Array	Lists the certificates. For details, see **Table 10-201**.
instance_num	Integer	Specifies the number of certificates.

Table 10-201 certificates parameter description

Parameter	Type	Description
id	String	Specifies the certificate ID.
tenant_id	String	Specifies the ID of the project where the certificate is used. The value contains a maximum of 255 characters.
admin_state_up	Boolean	Specifies the administrative status of the certificate. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
name	String	Specifies the certificate name. The value contains a maximum of 255 characters.
description	String	Provides supplementary information about the certificate. The value contains a maximum of 255 characters.
type	String	Specifies the certificate type. The value can be one of the following: • **server**: indicates the server certificate. • **client**: indicates the CA certificate.

Parameter	Type	Description
domain	String	Specifies the domain name associated with the server certificate. A domain name can contain up to 100 characters. You can specify up to 30 domain names and separate them using commas (,). The value can be one of the following: ● A common domain name contains 0 to 100 characters and consists of several labels separated by periods (.). Each label can contain a maximum of 63 characters, including letters, digits, and hyphens (-), and must start and end with a letter or digit. Example: www.test.com ● In addition to the requirements for common domain names, a wildcard domain name can start with an asterisk (*). Example: *.test.com **NOTE** ● This parameter is valid only when **type** is set to **server**.
private_key	String	Specifies the private key of the server certificate in PEM format.
certificate	String	Specifies the public key of the server certificate or CA certificate used to authenticate the client. The value of parameter **type** determines whether a public key or CA certificate is required. Both types of certificates are in PEM format.
expire_time	String	Specifies the time when the certificate expired. The UTC time is in *YYYY-MM-DD HH:MM:SS* format.
create_time	String	Specifies the time when the certificate was created. The UTC time is in *YYYY-MM-DD HH:MM:SS* format.
update_time	String	Specifies the time when the certificate was updated. The UTC time is in *YYYY-MM-DD HH:MM:SS* format.

Example Request

- Request example 1: Querying all certificates
  ```
  GET https://{Endpoint}/v2.0/lbaas/certificates
  ```


- Example 2: Querying a certificate whose ID is ef4d341365754a959556576501791b19 or ed40e8ea9957488ea82de025e35b74c0

```
GET https://{Endpoint}/v2.0/lbaas/certificates?
id=ef4d341365754a959556576501791b19&id=ed40e8ea9957488ea82de025e35b74c0
```

Example Response

- Example response 1


```
{
   "certificates": [
      {
         "certificate": "-----BEGIN CERTIFICATE-----
\nMIIC4TCCAcmgAwIBAgICEREwDQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXlD
\nb21wYW55IENBMB4XDTE4MDcwMjEzMjU0N1oXDTQ1MTExNzEzMjU0N1owFDESMBAG
\nA1UEAwwJbG9jYWxob3N0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA\n0FQGzi3ucTX
+DNud1p/
b4XVM6I3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5\nU0NqPQZKUrZz3rQeLN9mYiUTJZPutYlFDDb
B8CtlgV+eyU9yYJslWx/
Bm5kWNPh9\n7B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/W7jaS
\nIAzlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylYKy4zgnv1tn/K
\ny09cxLKAFtgoZWQD2FAZJf9F7k1kYNwqITz3CPlLZUUn7yw3nkOOtLMI28IEv0Wy
\nYd7CMJQkS1NPJBKNOGfR/wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29t
\nhwQKuUvJhwR/AAABMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCSqGSIb3DQEBCwUA
\nA4IBAQA8lMQJxaTey7EjXtRLSVlEAMftAQPG6jijNQuvIBQYUDauDT4W2XUZ5wAn
\njiOyQ83va672K1G9s8n6xlH+xwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDa
\nezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPRLYlzp1HMnI6hkjPk4PCZ
\nwKnha0dlScati9CCt3UzXSNJOSLalKdHErH08Iqd+1BchScxCfk0xNITn1HZZGmI\n
+vbmunok3A2lucI14rnsrcbkGYqxGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZ\niYsGDVN
+9QBd0eYUHce+77s96i3I\n-----END CERTIFICATE-----",
         "create_time": "2017-02-25 09:35:27",
         "expire_time": "2045-11-17 13:25:47",
         "description": "description for certificate",
         "domain": "www.elb.com",
         "id": "23ef9aad4ecb463580476d324a6c71af",
         "admin_state_up": true,
         "tenant_id": "a31d2bdcf7604c0faaddb058e1e08819",
         "name": "https_certificate",
         "private_key":
"-----BEGIN PRIVATE KEY-----
\nMIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDQVAbOLe5xNf4M
\n253Wn9vhdUzojetjv4J+B7kYwsMhRcgdcJ8KCnX1nfzTvI2ksXlTQ2o9BkpStnPe\ntB4s32ZiJRMlk
+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM
\nMD30gLh6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8Icq39buNpIgDOWzEP5AzqXt
\nCOFYn6RTH5SRug4hKNN7sT1eYMslHu7wtEBDKVgrLjOCe/W2f8rLT1zEsoAW2Chl\nZAPYUBkl/
0XuTWRg3CohPPcI+UtlRSfvLDeeQ460swjbwgS/RbJh3slwlCRLU08k\nEo04Z9H/
AgMBAAECggEAEIeaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/Hl
\nfvCArftGgMaYWPSNCJRMXB7tPwpQu19esjz4Z/cR2Je4fTLPrffGUsHFgZjv5OQB
\nZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr
\nciu9YkInNEHu6uRJ5g/eGGX3KQynTvVIhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M\nEGpfYI6AdHIwFZcT/
RNAxhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7Ale\nkrguPtfV1vWklg
+bUFhgGaiAEYTpAUN9t2DVIiijgQKBgQDnYMMsaF0r557CM1CT
\nXUqgCZo8MKeV2jf2drlxRRwRl33SksQbzAQ/qrLdT7GP3sCGqvkxWY2FPdFYf8kx
\nGcCeZPcIeZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/fbwjpjP7dt
\nJ7n8EzkRUNE6aIMHOFEeych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr
\niWgTWHXPZxUQaYhpjXo6+lMI6DpExiDgBAkMzJGIvS7yQiYWU+wthAr9urbWYdGZ
\nlS6VjoTkF6r7VZoILXX0fbuXh6lm8K8IQRfBpJff56p9phMwaBpDNDrfpHB5utBU
\nxs40yIdp6wKBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zJf3bGSXU/jR4eB
\n1lVQhELGI9CbKSdzKM71GyEImix/T7FnJSHIWlho1qVo6AQyduNWnAQD15pr8KAd
\nXGXAZZ1FQcb3KYa+2fflERmazdOTwjYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak\n/
735uP20KKqhNehZpC2dJei7OiIgRhCS/dKASUXHSW4fptBnUxACYocdDxtY4Vha\nfI7FPMdvGl8ioYbvlHFh
+X0Xs9r1S8yeWnHoXMb6eXWmYKMJrAoveLa+2cFm1Agf
\n7nLhA4R4lqm9IpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAJkD4wHW54Pwd4Ctfk9o
\njHjWB7pQlUYpTZO9dm+4fpCMn9Okf43AE2yAOaAP94GdzdDJkxfciXKcsYr9Iluk
\nfaoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BUlGKMWXzuEd\n3fy
+1rCUwzOp9LSjtJYf4ege\n-----END PRIVATE KEY-----",
         "type": "server",
         "update_time": "2017-02-25 09:35:27"
```



```
        }
    ],
    "instance_num": 1
}
```

- Example response 2

```
{
    "certificates": [
        {
            "description": "Push by SSL Certificate Manager",
            "domain": null,
            "id": "ed40e8ea9957488ea82de025e35b74c0",
            "name": "certForSonar9",
            "certificate": "-----BEGIN CERTIFICATE-----
MIIFizCCBHOgAwIBAgIQBlQycV3bWsVsCttvv5rgRjANBgkqhkiG9w0BAQsFADBu
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMS0wKwYDVQQDEyRFbmNyeXB0aW9uIEV2ZXJ5d2hlcmUg
RFYgVExTIENBIC0gRzEwHhcNMTgwNzEwMDAwMDAwWhcNMTkwNzEwMTIwMDAwWjAU
MRIwEAYDVQQDEwlpY2UxMjMudGswggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQCtTDlQMoAvyInR6X1dihhNwbdGesbMW6NZX7ffpj9XrB3KCqqlxzI4VmH9
PntvrpLJNeolgLqDZZc4zKbUkmqxY1dvGDs41coKzdtc9Ig23GVK48wfesnk5r50
afyU52R1JlSHDOhiDhHOSyhrOzc2GreLrByWKFUaAue6rTnyMbzQaSPtrTAqsURZ
wcmJ6R3A6JwokOgxXBSu41ufPQiFkMgxygKxEBLzIJLjRqCXQHYoxbsTyolb6jwp
w4H6vcRIEcFAgs98ApWRoEKjy7eOP3UUm05F+OkOvXhrlxEqIPm/rlwE0PmVlmm9
DgBafYb3xT/MtT2VRSfCJQHgIcsdAgMBAAGjggJ9MIICeTAfBgNVHSMEGDAWgBRV
dE+yck/1YLpQ0dfmUVyaAYca1zAdBgNVHQ4EFgQUEFavzYXBNbIHBchbaKcUKad+
qCEwIwYDVR0RBBwwGoIJaWNlMTIzLnRrgg13d3cuaWNlMTIzLnRrMA4GA1UdDwEB
/wQEAwIFoDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwTAYDVR0gBEUw
QzA3BglghkgBhv1sAQIwKjAoBggrBgEFBQcCARYcaHR0cHM6Ly93d3cuZGlnaWNl
cnQuY29tL0NQUzAIBgZngQwBAgEwgYEGCCsGAQUFBwEBBHUwczAlBggrBgEFBQcw
AYYZaHR0cDovL29jc3AyLmRpZ2ljZXJ0LmNvbTBKBggrBgEFBQcwAoY+aHR0cDov
L2NhY2VydHMuZGlnaWNlcnQuY29tL0VuY3J5cHRpb25FdmVyeXdoZXJlRFZUTFND
QS1HMS5jcnQwCQYDVR0TBAIwADCCAQQGCisGAQQB1nkCBAIEgfUEgfIA8AB2AKS5
CZC0GFgUh7sTosxncAo8NZgE+RvfuON3zQ7IDdwQAAABZIOnLCIAAAQDAEcwRQIh
AJX6gCXNggPdfOFdDtZPzlYr64TTrR/+b9QKKhyJ2EjBAiAWgu3BG2QK9tWQXpUN
IFadc0nvqmDovabg5nmRMan2mQB2AId1v+dZfPiMQ5lfvfNu/1aNR1Y2/0q1YMG0
6v9eoIMPAAABZIOnLQEAAAQDAEcwRQIhAJVRe/7n88dD6KdhNrd4LdFjGARQNmta
Y/K2dFDOXPSfAiBOLrWW8unHOL25RWHJU7Ost3XkNhQYtrLDJrnzo/9kZzANBgkq
hkiG9w0BAQsFAAOCAQEAeqtX9cHmj4OnNAk0IGmF3nKS/u/UgGsY4EJfXwQY2bTZ
PCkqxQOA6HEx59vJ+UilTojrNDi0WskRm/8SKBHtmRwzwX3ile8KiR6fFfQhPUtV
XHZcTfAFo47c7axqon8vumMlEv1PxVImivQ446K7z3kGm34dhMYxS4Gz2gTl8IKt
90OegejuhbAs5Wlvp1BK8HlYIb5+mw+cgkUC9KTALs5qVbWzogb0bS20KaYarGcu
otcZAOMeJdBFWnpzhr1fxmjaNY4u4hrgPZSTU/iBjdHapoza3zAFfxysmGYqs9dR
jFyxZeR4scz8GqSTFviNdH9jvtDJkdAC5hfMaB811Q==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEqjCCA5KgAwIBAgIQAnmsRYvBskWr+YBTzSybsTANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0xNzExMjcxMjQ2MTBaFw0yNzExMjcxMjQ2MTBaMG4xCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j
b20xLTArBgNVBAMTJEVuY3J5cHRpb24gRXZlcnl3aGVyZSBEViBUTFMgQ0EgLSBH
MTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALPeP6wkab41dyQh6mKc
oHqt3jRIxW5MDvf9QyiOR7VfFwK656es0UFiIb74N9pRntzF1UgYzDGu3ppZVMdo
lbxhm6dWS9OK/lFehKNT0OYI9aqk6F+U7cA6jxSC+iDBPXwdF4rs3KRyp3aQn6pj
pp1yr7IB6Y4zv72Ee/PlZ/6rK6InC6WpK0nPVOYR7n9iDuPe1E4IxUMBH/T33+3h
yuH3dvfgiWUOUkjdpMbyxX+XNle5uEIiyBsi4IvbcTCh8ruifCIi5mDXkZrnMT8n
wfYCV6v6kDdXkbgGRLKsR4pucbJtbKqIkUGxuZI2t7pfewKRc5nWecvDBZf3+p1M
pA8CAwEAAaOCAU8wggFLMB0GA1UdDgQWBBRVdE+yck/1YLpQ0dfmUVyaAYca1zAf
BgNVHSMEGDAWgBQD3lA1VtFMu2bwo+IbG8OXsj3RVTAOBgNVHQ8BAf8EBAMCAYYw
HQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMBIGA1UdEwEB/wQIMAYBAf8C
AQAwNAYIKwYBBQUHAQEEKDAmMCQGCCsGAQUFBzABhhhodHRwOi8vb2NzcC5kaWdp
Y2VydC5jb20wQgYDVR0fBDswOTA3oDWgM4YxaHR0cDovL2NybDMuZGlnaWNlcnQu
Y29tL0RpZ2lDZXJ0R2xvYmFsUm9vdENBLmNybDBMBgNVHSAERTBDMDcGCWCGSAGG
/WwBAjAqMCgGCCsGAQUFBwIBFhxodHRwczovL3d3dy5kaWdpY2VydC5jb20vQ1BT
MAgGBmeBDAECATANBgkqhkiG9w0BAQsFAAOCAQEAK3Gp6/aGq7aBZsxf/oQ+TD/B
SwW3AU4ETK+GQf2kFzYZkby5SFrHdPomunx2HBzViUchGoofGgg7gHW0W3MlQAXW
M0r5LUvStcr82QDWYNPaUy4taCQmyaJ+VB+6wxHstSigOlSNF2a6vg4rgexixeiV
4YSB03Yqp2t3TeZHM9ESfkus74nQyW7pRGezj+TC44xCagCQQOzzNmzEAP2SnCrJ
sNE2DpRVMnL8J6xBRdjmOsC3N6cQuKuRXbzByVBjCqAA8t1L0I+9wXJerLPyErjy
```

rMKWaBFLmfK/AHNF4ZihwPGOc7w6UHczBZXH5RFzJNnww+WnKuTPI0HfnVH8lg==
-----END CERTIFICATE-----",
            "type": "server",
            "create_time": "2019-03-03 16:32:30",
            "private_key": "-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEArUw5UDKAL8iJ0el9XYoYTcG3RnrGzFujWV+336Y/V6wdygqq
pccyOFZh/T57b66SyTXqJYC6g2WXOMym1JJqsWNXbxg7ONXKCs3bXPSINtxlSuPM
H3rJ5Oa+dGn8lOdkdSZUhwzoYg4Rzksoazs3Nhq3i6wclihVGgLnuq058jG80Gkj
7a0wKrFEWcHJiekdwOicKJDoMVwUruNbnz0IhZDIMcoCsRAS8yCS40agl0B2KMW7
E8qJW+o8KcOB+r3ESBHBQILPfAKVkaBCo8u3jj91FJtORfjpDr14a5cRKiD5v65c
BND5lZZpvQ4AWn2G98U/zLU9lUUnwiUB4CHLHQIDAQABAoIBAGs5rISompP2OwA8
virwVRVXdPUQ5oxvbuTPys+A59RxVIU8kFW+qJ4fJMYysOFrXLtOtq+5tK20YBru
1ZLVfVqAowrELXB/J2ID+WTMkLORLsNlq1kW+nC9LL6PDY98lLW/n7FoFSkGl5HT
AxFGNGUvpr2vIojuL6nGfmcM47uscJ9aP6IJxr4p70dhPVjZBdnMnXYwRkB3dZt/
E0B/p8J5i3oo5Rucv4DOfB+01wXGAVyx5/zce+NZdhyrivkj3hHV55SxGhVWzWhj
a3dAlbpKwYgfILj0inRdJYmIjBdbGb2HFix7+ncBg8B2oerJXC6/fANwRGu5/LZU
5xuPVWkCgYEA6an8TY1unIGLYL5aBJ16Tx4usqMyTXr/T4zkQyftRPMt+ZuxVQHl
GHsg7XvLFNd04MBZXtkZXaYVcpOm7OUYcl0i9ZAkWXXoXcBtn1Oom3gz/7RjAUnp
k+myvxCUSQ2JSz4u3QBtyPVyYNyBFXrKqdKfcYyG85+yQVHBNMVrdvMCgYEAvd0C
hFpm83ha+VQp+9XN1DYZNUyqhibj/E3X9jAn+gDbzlKxw/D9en2RIlQYUrl8+il8
QKk4cfOxJYStQfxptz8QBPVeLajDN67zJ0Rk8AB50HHHcNSU8uFkaO8KxsyVjbLS
+JltqfJAEraXLinbp1Fxcg9DsQdMd6cw2DmrWa8CgYEA1UjJOUzo80i4HYWDC4Vn
OEK3o22do+WqmEVlsfsG9BH5HEdGVe7V3EO/6aY+1/ZXBDPvH8mRAs9v8lbeXow7
hWClYZfB5jre8HyOU4l8dPUCmdxhJrL913rRIuASSqBlet32ztnuXCnWzp1X4nBj
/yF3UqFQKZ7SihcDAZVWo4sCgYEAj7al/BcNzIcynX2mldhdh583b4/Ll+YCNm2Z
5eDHscZKmx8fLcjRpZE8dXagPqXmwtj6E1vDvQWP9m06VDNCthFHB+nO0tLmidSk
evmbScuiaTRmmbJf2IThY0hlqNsc7PgKF2DTkIstEr0hLDFE8Z6FN6f0PiDfMcbd
Ax6L5EMCgYEA0+qhuQftKQkGdbXX9r3H8N0TVh27ByfL3kKVYy0dUJMvsOAq6d97
8mEhYhrYt88f1sFsPM7G09XpCcBXwiKxw8+CDt9auD4r1snBnILpqMPmanF4UDXH
L7s+4it+nIQy24P6g1PihtzsM+HD2UCErBiYUJdRK8Q9GGHdZojFk9Y=
-----END RSA PRIVATE KEY-----
",
            "update_time": "2019-03-03 16:32:30",
            "admin_state_up": true,
            "tenant_id": "601240b9c5c94059b63d484c92cfe308",
            "expire_time": "2019-07-10 12:00:00"
        },
        {
            "description": null,
            "domain": "www.elb.com",
            "id": "ef4d341365754a959556576501791b19",
            "name": "certificate_28b824c8bbee419992fb7974b2911c72",
            "certificate": "-----BEGIN CERTIFICATE-----
MIIDpTCCAo2gAwIBAgIJAKdmmOBYnFvoMA0GCSqGSIb3DQEBCwUAMGkxCzAJBgNV
BAYTAnh4MQswCQYDVQQIDAJ4eDELMAkGA1UEBwwCeHgxCzAJBgNVBAoMAnh4MQsw
CQYDVQQLDAJ4eDELMAkGA1UEAwwCeHgxGTAXBgkqhkiG9w0BCQEWCnh4QDE2My5j
b20wHhcNMTcxMjA0MDM0MjQ5WhcNMjAxMjAzMDM0MjQ5WjBpMQswCQYDVQQGEwJ4
eDELMAkGA1UECAwCeHgxCzAJBgNVBAcMAnh4MQswCQYDVQQKDAJ4eDELMAkGA1UE
CwwCeHgxCzAJBgNVBAMMAnh4MRkwFwYJKoZIhvcNAQkBFgp4eEAxNjMuY29tMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwZ5UJULAjWr7p6FVwGRQRjFN
2s8tZ/6LC3X82fajpVsYqF1xqEuUDndDXVD09E4u83MS6HO6a3bIVQDp6/klnYld
iE6Vp8HH5BSKaCWKVg8lGWg1UM9wZFnlryi14KgmpIFmcu9nA8yV/6MZAe6RSDmb
3iyNBmiZ8aZhGw2pI1YwR+15MVqFFGB+7ExkziROi7L8CFCyCezK2/oOOvQsH1dz
Q8z1JXWdg8/9Zx7Ktvgwu5PQM3cJtSHX6iBPOkMU8Z8TugLlTqQXKZOEgwajwvQ5
mf2DPkVgM08XAgaLJcLigwD513koAdtJd5v+9irw+5LAuO3JclqwTvwy7u/YwwID
AQABo1AwTjAdBgNVHQ4EFgQUo5A2tIu+bcUfvGTD7wmEkhXKFjcwHwYDVR0jBBgw
FoAUo5A2tIu+bcUfvGTD7wmEkhXKFjcwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0B
AQsFAAOCAQEAWJ2rS6Mvlqk3GfEpboezx2J3X7l1z8Sxoqg6ntwB+rezvK3mc9H0
83qcVeUcoH+0A0lSHyFN4FvRQL6X1hEheHarYwJK4agb231vb5erasuGO463eYEG
r4SfTuOm7SyiV2xxbaBKrXJtpBp4WLL/s+LF+nklKjaOxkmxUX0sM4CTA7uFJypY
c8Tdr8lDDNqoUtMD8BrUCJi+7lmMXRcC3Qi3oZJW76ja+kZA5mKVFPd1ATih8TbA
i34R7EQDtFeiSvBdeKRsPp8c0KT8H1B4lXNkkCQs2WX5p4lm99+ZtLD4glw8x6Ic
i1YhgnQbn5E0hz55OLu5jvOkKQjPCW+8Kg==
-----END CERTIFICATE-----",
            "type": "server",
            "create_time": "2018-09-28 03:00:47",
            "private_key": "-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAwZ5UJULAjWr7p6FVwGRQRjFN2s8tZ/6LC3X82fajpVsYqF1x
qEuUDndDXVD09E4u83MS6HO6a3bIVQDp6/klnYldiE6Vp8HH5BSKaCWKVg8lGWg1


```
UM9wZFnlryi14KgmpIFmcu9nA8yV/6MZAe6RSDmb3iyNBmiZ8aZhGw2pI1YwR+15
MVqFFGB+7ExkziROi7L8CFCyCezK2/oOOvQsH1dzQ8z1JXWdg8/9Zx7Ktvgwu5PQ
M3cJtSHX6iBPOkMU8Z8TugLlTqQXKZOEgwajwvQ5mf2DPkVgM08XAgaLJcLigwD5
13koAdtJd5v+9irw+5LAuO3JclqwTvwy7u/YwwIDAQABAoIBACU9S5fjD9/jTMXA
DRs08A+gGgZUxLn0xk+NAPX3LyB1tfdkCaFB8BccLzO6h3KZuwQOBPv6jkdvEDbx
Nwyw3eA/9GJsIvKiHc0rejdvyPymaw9I8MA7NbXHaJrY7KpqDQyk6sx+aUTcy5jg
iMXLWdwXYHhJ/1HVOo603oZyiS6HZeYU089NDUcX+1SJi3e5Ke0gPVXEqCq1O11/
rh24bMxnwZo4PKBWdcMBN5Zf/4ij9vrZE+fFzW7vGBO48A5lvZxWU2U5t/OZQRtN
1uLOHmMFa0FIF2aWbTVfwdUWAFsvAOkHj9VV8BXOUwKOUuEktdkfAlvrxmsFrO/H
yDeYYPkCgYEA/S55CBbR0sMXpSZ56uRn8JHApZJhgkgvYr+FqDUq/e92nAzf01P
RoEBUajwrnf1ycevN/SDfbtWzq2XJGqhWdJmtpO16b7KBsC6BdRcH6dnOYh31jgA
vABMIP3wzl4zSVTyxRE8LDuboytF1mSCeV5tHYPQTZNwrplDnLQhywcCgYEAw8Yc
Uk/eiFr3hfH/ZohMfV5p82Qp7DNIGRzw8YtVG/3+vNXrAXW1VhugNhQY6L+zLtJC
aKn84ooup0m3YCg0hvINqJuvzfsuzQgtjTXyaE0cEwsjUusOmiuj09vVx/3U7siK
Hdjd2ICPCvQ6Q8tdi8jV320gMs05AtaBkZdsiWUCgYEAtLw4Kk4f+xTKDFsrLUNf
75wcqhWVBiwBp7yQ7UX4EYsJPKZcHMRTk0EEcAbpyaJZE3I44vjp5ReXIHNLMfPs
uvI34J4Rfot0LN3n7cFrAi2+wpNo+MOBwrNzpRmijGP2uKKrq4JiMjFbKV/6utGF
Up7VxfwS904JYpqGaZctiIECgYA1A6nZtF0riY6ry/uAdXpZHL8ONNqRZtWoT0kD
79otSVu5ISiRbaGcXsDExC52oKrSDAgFtbqQUiEOFg09UcXfoR6HwRkba2CiDwve
yHQLQI5Qrdxz8Mk0gIrNrSM4FAmcW9vi9z4kCbQyoC5C+4gqeUlRpDIkQBWP2Y4
2ct/bQKBgHv8qCsQTZphOxc31BJPa2xVhuv18cEU3XLUrVfUZ/1f43JhLp7gynS2
ep++LKUi9D0VGXY8bqvfJjbECoCeu85vl8NpCXwe/LoVoIn+7KaVIZMwqoGMfgNl
nEqm7HWkNxHhf8A6En/IjleuddS1sf9e/x+TJN1Xhnt9W6pe7Fk1
-----END RSA PRIVATE KEY-----",
            "update_time": "2018-09-28 03:00:47",
            "admin_state_up": true,
            "tenant_id": "601240b9c5c94059b63d484c92cfe308",
            "expire_time": "2020-12-03 03:42:49"
        }
    ],
    "instance_num": 2
}
```


Status Code

For details, see **Status Codes**.

10.1.9.3 Querying Details of a Certificate

Function

This API is used to query details about a certificate.

URI

GET /v2.0/lbaas/certificates/{certificate_id}

Table 10-202 Parameter description

Parameter	Mandatory	Type	Description
certificate_id	Yes	String	Specifies the certificate ID.

Request

None

Response

Table 10-203 Parameter description

Parameter	Type	Description
id	String	Specifies the certificate ID.
tenant_id	String	Specifies the ID of the project where the certificate is used. The value contains a maximum of 255 characters.
admin_state_up	Boolean	Specifies the administrative status of the certificate. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
name	String	Specifies the certificate name. The value contains a maximum of 255 characters.
description	String	Provides supplementary information about the certificate. The value contains a maximum of 255 characters.
type	String	Specifies the certificate type. The value can be one of the following: • **server**: indicates the server certificate. • **client**: indicates the CA certificate.

Parameter	Type	Description
domain	String	Specifies the domain name associated with the server certificate. A domain name can contain up to 100 characters. You can specify up to 30 domain names and separate them using commas (,). The value can be one of the following: ● A common domain name contains 0 to 100 characters and consists of several labels separated by periods (.). Each label can contain a maximum of 63 characters, including letters, digits, and hyphens (-), and must start and end with a letter or digit. Example: www.test.com ● In addition to the requirements for common domain names, a wildcard domain name can start with an asterisk (*). Example: *.test.com **NOTE** ● This parameter is valid only when **type** is set to **server**.
private_key	String	Specifies the private key of the server certificate in PEM format.
certificate	String	Specifies the public key of the server certificate or CA certificate used to authenticate the client. The value of parameter **type** determines whether a public key or CA certificate is required. Both types of certificates are in PEM format.
expire_time	String	Specifies the time when the certificate expired. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format.
create_time	String	Specifies the time when the certificate was created. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format.
update_time	String	Specifies the time when the certificate was updated. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format.

Example Request

- Example request: Querying details of a certificate
  GET https://{Endpoint}/v2.0/lbaas/certificates/23ef9aad4ecb463580476d324a6c71af

Example Response

- Example response


```
{
    "certificate":
"-----BEGIN CERTIFICATE-----
\nMIIC4TCCAcmgAwIBAgICEREwDQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXlD
\nb21wYW55IENBMB4XDTE4MDcwMjEzMjU0N1oXDTQ1MTExNzEzMjU0N1owFDESMBAG
\nA1UEAwwJbG9jYWxob3N0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
\n0FQGzi3ucTX+DNud1p/b4XVM6l3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5
\nU0NqPQZKUrZz3rQeLN9mYiUTJZPutYlFDDbB8CtlgV+eyU9yYJslWx/Bm5kWNPh9
\n7B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/W7jaS
\nIAzlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylYKy4zgnv1tn/K
\ny09cxLKAFtgoZWQD2FAZJf9F7k1kYNwqITz3CPlLZUUn7yw3nkOOtLMI28IEv0Wy
\nYd7CMJQkS1NPJBKNOGfR/wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29t
\nhwQKuUvJhwR/AAABMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCSqGSIb3DQEBCwUA
\nA4IBAQA8lMQJxaTey7EjXtRLSVlEAMftAQPG6jijNQuvIBQYUDauDT4W2XUZ5wAn
\njiOyQ83va672K1G9s8n6xlH+xwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDa
\nezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPRLYlzp1HMnI6hkjPk4PCZ
\nwKnha0dlScati9CCt3UzXSNJOSLalKdHErH08Iqd+1BchScxCfk0xNITn1HZZGmI
\n+vbmunok3A2lucI14rnsrcbkGYqxGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZ
\niYsGDVN+9QBd0eYUHce+77s96i3I
\n-----END CERTIFICATE-----",
    "create_time": "2017-02-25 09:35:27",
    "expire_time": "2045-11-17 13:25:47",
    "description": "description for certificate",
    "domain": "www.elb.com",
    "id": "23ef9aad4ecb463580476d324a6c71af",
    "tenant_id": "a31d2bdcf7604c0faaddb058e1e08819",
    "admin_state_up": true,
    "name": "https_certificate",
    "private_key":
"-----BEGIN PRIVATE KEY-----
\nMIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDQVAbOLe5xNf4M
\n253Wn9vhdUzojetjv4J+B7kYwsMhRcgdcJ8KCnX1nfzTvI2ksXlTQ2o9BkpStnPe
\ntB4s32ZiJRMlk+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM
\nMD30gLh6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8Icq39buNpIgDOWzEP5AzqXt
\nCOFYn6RTH5SRug4hKNN7sT1eYMslHu7wtEBDKVgrLjOCe/W2f8rLT1zEsoAW2Chl
\nZAPYUBkl/0XuTWRg3CohPPcI+UtlRSfvLDeeQ460swjbwgS/RbJh3slwlCRLU08k
\nEo04Z9H/AgMBAAECggEAEIeaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/Hl
\nfvCArftGgMaYWPSNCJRMXB7tPwpQu19esjz4Z/cR2Je4fTLPrffGUsHFgZjv5OQB
\nZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr
\nciu9YkInNEHu6uRJ5g/eGGX3KQynTvVIhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M
\nEGpfYI6AdHIwFZcT/RNAxhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7Ale
\nkrguPtfV1vWklg+bUFhgGaiAEYTpAUN9t2DVIiijgQKBgQDnYMMsaF0r557CM1CT
\nXUqgCZo8MKeV2jf2drlxRRwRl33SksQbzAQ/qrLdT7GP3sCGqvkxWY2FPdFYf8kx
\nGcCeZPcIeZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/fbwjpjP7dt
\nJ7n8EzkRUNE6aIMHOFEeych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr
\niWgTWHXPZxUQaYhpjXo6+lMI6DpExiDgBAkMzJGIvS7yQiYWU+wthAr9urbWYdGZ
\nlS6VjoTkF6r7VZoILXX0fbuXh6lm8K8IQRfBpJff56p9phMwaBpDNDrfpHB5utBU
\nxs40yIdp6wKBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zJf3bGSXU/jR4eB
\n1lVQhELGI9CbKSdzKM71GyEImix/T7FnJSHIWlho1qVo6AQyduNWnAQD15pr8KAd
\nXGXAZZ1FQcb3KYa+2fflERmazdOTwjYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak
\n/735uP20KKqhNehZpC2dJei7OiIgRhCS/dKASUXHSW4fptBnUxACYocdDxtY4Vha
\nfI7FPMdvGl8ioYbvlHFh+X0Xs9r1S8yeWnHoXMb6eXWmYKMJrAoveLa+2cFm1Agf
\n7nLhA4R4lqm9IpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAJkD4wHW54Pwd4Ctfk9o
\njHjWB7pQlUYpTZO9dm+4fpCMn9Okf43AE2yAOaAP94GdzdDJkxfciXKcsYr9IIuk
\nfaoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BUlGKMWXzuEd
\n3fy+1rCUwzOp9LSjtJYf4ege
\n-----END PRIVATE KEY-----",
    "type": "server",
    "update_time": "2017-02-25 09:35:27"
}
```


Status Code

For details, see **Status Codes**.

10.1.9.4 Updating a Certificate

Function

This API is used to update a certificate.

URI

PUT /v2.0/lbaas/certificates/{certificate_id}

Table 10-204 Parameter description

Parameter	Mandatory	Type	Description
certificate_id	Yes	String	Specifies the certificate ID.

Request

Table 10-205 Parameter description

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Specifies the administrative status of the certificate. This parameter is reserved, and the default value is **true**.
name	No	String	Specifies the certificate name. The value contains a maximum of 255 characters.
description	No	String	Provides supplementary information about the certificate. The value contains a maximum of 255 characters.

Parameter	Mandatory	Type	Description
domain	No	String	Specifies the domain name associated with the server certificate. A domain name can contain up to 100 characters. You can specify up to 30 domain names and separate them using commas (,). The value can be one of the following: ● A common domain name contains 0 to 100 characters and consists of several labels separated by periods (.). Each label can contain a maximum of 63 characters, including letters, digits, and hyphens (-), and must start and end with a letter or digit. Example: www.test.com ● In addition to the requirements for common domain names, a wildcard domain name can start with an asterisk (*). Example: *.test.com **NOTE** ● This parameter is valid only when **type** is set to **server**.
private_key	No	String	Specifies the private key of the server certificate. The value must be PEM encoded. ● This parameter will be ignored if **type** is set to **client**. A CA server can still be created and used normally. This parameter will be left blank even if you enter a private key that is not PEM encoded. ● This parameter is valid and mandatory only when **type** is set to **server**. If you enter an invalid private key, an error is returned.
certificate	No	String	Specifies the public key of the server certificate or CA certificate used to authenticate the client. The value of parameter **type** determines whether a public key or CA certificate is required. The public key is in PEM format.

Response

Table 10-206 Parameter description

Parameter	Type	Description
id	String	Specifies the certificate ID.
tenant_id	String	Specifies the ID of the project where the certificate is used. The value contains a maximum of 255 characters.
admin_state_up	Boolean	Specifies the administrative status of the certificate. This parameter is reserved. The value can be **true** or **false**. • **true**: Enabled • **false**: Disabled
name	String	Specifies the certificate name. The value contains a maximum of 255 characters.
description	String	Provides supplementary information about the certificate. The value contains a maximum of 255 characters.
type	String	Specifies the certificate type. The value can be one of the following: • **server**: indicates the server certificate. • **client**: indicates the CA certificate.

Parameter	Type	Description
domain	String	Specifies the domain name associated with the server certificate. A domain name can contain up to 100 characters. You can specify up to 30 domain names and separate them using commas (,). The value can be one of the following: ● A common domain name contains 0 to 100 characters and consists of several labels separated by periods (.). Each label can contain a maximum of 63 characters, including letters, digits, and hyphens (-), and must start and end with a letter or digit. Example: www.test.com ● In addition to the requirements for common domain names, a wildcard domain name can start with an asterisk (*). Example: *.test.com **NOTE** ● This parameter is valid only when **type** is set to **server**.
private_key	String	Specifies the private key of the server certificate in PEM format.
certificate	String	Specifies the public key of the server certificate or CA certificate used to authenticate the client. The value of parameter **type** determines whether a public key or CA certificate is required. Both types of certificates are in PEM format.
expire_time	String	Specifies the time when the certificate expired. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format.
create_time	String	Specifies the time when the certificate was created. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format.
update_time	String	Specifies the time when the certificate was updated. The UTC time is in *YYYY-MM-DDTHH:MM:SS* format.

Example Request

- Example request: Updating a certificate
  ```
  PUT https://{Endpoint}/v2.0/lbaas/certificates/23ef9aad4ecb463580476d324a6c71af
  ```



```
{
   "certificate":
"-----BEGIN CERTIFICATE-----
\nMIIC4TCCAcmgAwIBAgICEREwDQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXlD
\nb21wYW55IENBMB4XDTE4MDcwMjEzMjU0N1oXDTQ1MTExNzEzMjU0N1owFDESMBAG
\nA1UEAwwJbG9jYWxob3N0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
\n0FQGzi3ucTX+DNud1p/b4XVM6I3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5
\nU0NqPQZKUrZz3rQeLN9mYiUTJZPutYlFDDbB8CtlgV+eyU9yYJslWx/Bm5kWNPh9
\n7B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/W7jaS
\nIAzlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylYKy4zgnv1tn/K
\ny09cxLKAFtgoZWQD2FAZJf9F7k1kYNwqITz3CPlLZUUn7yw3nkOOtLMI28IEv0Wy
\nYd7CMJQkS1NPJBKNOGfR/wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29t
\nhwQKuUvJhwR/AAABMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCSqGSIb3DQEBCwUA
\nA4IBAQA8lMQJxaTey7EjXtRLSVlEAMftAQPG6jijNQuvIBQYUDauDT4W2XUZ5wAn
\njiOyQ83va672K1G9s8n6xlH+xwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDa
\nezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPRLYlzp1HMnI6hkjPk4PCZ
\nwKnha0dlScati9CCt3UzXSNJOSLalKdHErH08Iqd+1BchScxCfk0xNITn1HZZGmI
\n+vbmunok3A2lucI14rnsrcbkGYqxGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZ
\niYsGDVN+9QBd0eYUHce+77s96i3I
\n-----END CERTIFICATE-----",
   "description": "description for certificate",
   "domain": "www.elb.com",
   "name": "https_certificate",
   "private_key":
"-----BEGIN PRIVATE KEY-----
\nMIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDQVAbOLe5xNf4M
\n253Wn9vhdUzojetjv4J+B7kYwsMhRcgdcJ8KCnX1nfzTvI2ksXlTQ2o9BkpStnPe
\ntB4s32ZiJRMlk+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM
\nMD30gLh6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8Icq39buNpIgDOWzEP5AzqXt
\nCOFYn6RTH5SRug4hKNN7sT1eYMslHu7wtEBDKVgrLjOCe/W2f8rLT1zEsoAW2Chl
\nZAPYUBkl/0XuTWRg3CohPPcI+UtlRSfvLDeeQ460swjbwgS/RbJh3slwlCRLU08k
\nEo04Z9H/AgMBAAECggEAEIeaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/Hl
\nfvCArftGgMaYWPSNCJRMXB7tPwpQu19esjz4Z/cR2Je4fTLPrffGUsHFgZjv5OQB
\nZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr
\nciu9YkInNEHu6uRJ5g/eGGX3KQynTvVIhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M
\nEGpfYI6AdHIwFZcT/RNAxhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7Ale
\nkrguPtfV1vWklg+bUFhgGaiAEYTpAUN9t2DVIiijgQKBgQDnYMMsaF0r557CM1CT
\nXUqgCZo8MKeV2jf2drlxRRwRl33SksQbzAQ/qrLdT7GP3sCGqvkxWY2FPdFYf8kx
\nGcCeZPcIeZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/fbwjpjP7dt
\nJ7n8EzkRUNE6aIMHOFEeych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr
\niWgTWHXPZxUQaYhpjXo6+lMI6DpExiDgBAkMzJGIvS7yQiYWU+wthAr9urbWYdGZ
\nlS6VjoTkF6r7VZoILXX0fbuXh6lm8K8IQRfBpJff56p9phMwaBpDNDrfpHB5utBU
\nxs40yIdp6wKBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zJf3bGSXU/jR4eB
\n1lVQhELGI9CbKSdzKM71GyEImix/T7FnJSHIWlho1qVo6AQyduNWnAQD15pr8KAd
\nXGXAZZ1FQcb3KYa+2fflERmazdOTwjYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak
\n/735uP20KKqhNehZpC2dJei7OiIgRhCS/dKASUXHSW4fptBnUxACYocdDxtY4Vha
\nfI7FPMdvGl8ioYbvlHFh+X0Xs9r1S8yeWnHoXMb6eXWmYKMJrAoveLa+2cFm1Agf
\n7nLhA4R4lqm9IpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAJkD4wHW54Pwd4Ctfk9o
\njHjWB7pQlUYpTZO9dm+4fpCMn9Okf43AE2yAOaAP94GdzdDJkxfciXKcsYr9IIuk
\nfaoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BUlGKMWXzuEd
\n3fy+1rCUwzOp9LSjtJYf4ege
\n-----END PRIVATE KEY-----"
}
```


Example Response

- Example response


```
{
   "certificate": "-----BEGIN CERTIFICATE-----
\nMIIC4TCCAcmgAwIBAgICEREwDQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXlD
\nb21wYW55IENBMB4XDTE4MDcwMjEzMjU0N1oXDTQ1MTExNzEzMjU0N1owFDESMBAG
\nA1UEAwwJbG9jYWxob3N0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA\n0FQGzi3ucTX
+DNud1p/
b4XVM6I3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5\nU0NqPQZKUrZz3rQeLN9mYiUTJZPutYlFDDb
B8CtlgV+eyU9yYJslWx/
Bm5kWNPh9\n7B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/W7jaS
\nIAzlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylYKy4zgnv1tn/K
\ny09cxLKAFtgoZWQD2FAZJf9F7k1kYNwqITz3CPlLZUUn7yw3nkOOtLMI28IEv0Wy
\nYd7CMJQkS1NPJBKNOGfR/wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29t
```


\nhwQKuUvJhwR/AAABMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCSqGSIb3DQEBCwUA
\nA4IBAQA8lMQJxaTey7EjXtRLSVlEAMftAQPG6jijNQuvIBQYUDauDT4W2XUZ5wAn
\njiOyQ83va672K1G9s8n6xlH+xwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDa
\nezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPRLYlzp1HMnI6hkjPk4PCZ
\nwKnha0dlScati9CCt3UzXSNJOSLalKdHErH08Iqd+1BchScxCfk0xNITn1HZZGmI\n
+vbmunok3A2lucI14rnsrcbkGYqxGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZ\niYsGDVN
+9QBd0eYUHce+77s96i3l\n-----END CERTIFICATE-----",
"expire_time": "2045-11-17 13:25:47",
"create_time": "2017-02-25 09:35:27",
"description": "description for certificate",
"domain": "www.elb.com",
"id": "23ef9aad4ecb463580476d324a6c71af",
"admin_state_up": true,
"tenant_id": "a31d2bdcf7604c0faaddb058e1e08819",
"name": "https_certificate",
"private_key": "-----BEGIN PRIVATE KEY-----
\nMIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDQVAbOLe5xNf4M
\n253Wn9vhdUzojetjv4J+B7kYwsMhRcgdcJ8KCnX1nfzTvI2ksXlTQ2o9BkpStnPe
\ntB4s32ZiJRMlk+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM
\nMD30gLh6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8Icq39buNpIgDOWzEP5AzqXt
\nCOFYn6RTH5SRug4hKNN7sT1eYMslHu7wtEBDKVgrLjOCe/W2f8rLT1zEsoAW2Chl
\nZAPYUBkl/0XuTWRg3CohPPcI+UtlRSfvLDeeQ460swjbwgS/RbJh3slwlCRLU08k
\nEo04Z9H/AgMBAAECggEAEIeaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/Hl
\nfvCArftGgMaYWPSNCJRMXB7tPwpQu19esjz4Z/cR2Je4fTLPrffGUsHFgZjv5OQB
\nZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr
\nciu9YkInNEHu6uRJ5g/eGGX3KQynTvVIhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M
\nEGpfYI6AdHIwFZcT/RNAxhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7Ale
\nkrguPtfV1vWklg+bUFhgGaiAEYTpAUN9t2DVIiijgQKBgQDnYMMsaF0r557CM1CT
\nXUqgCZo8MKeV2jf2drlxRRwRl33SksQbzAQ/qrLdT7GP3sCGqvkxWY2FPdFYf8kx
\nGcCeZPcIeZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/fbwjpjP7dt
\nJ7n8EzkRUNE6aIMHOFEeych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr
\niWgTWHXPZxUQaYhpjXo6+lMI6DpExiDgBAkMzJGIvS7yQiYWU+wthAr9urbWYdGZ
\nlS6VjoTkF6r7VZoILXX0fbuXh6lm8K8IQRfBpJff56p9phMwaBpDNDrfpHB5utBU
\nxs40yIdp6wKBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zJf3bGSXU/jR4eB
\n1lVQhELGI9CbKSdzKM71GyEImix/T7FnJSHIWlho1qVo6AQyduNWnAQD15pr8KAd
\nXGXAZZ1FQcb3KYa+2fflERmazdOTwjYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak
\n/735uP20KKqhNehZpC2dJei7OiIgRhCS/dKASUXHSW4fptBnUxACYocdDxtY4Vha
\nfI7FPMdvGl8ioYbvlHFh+X0Xs9r1S8yeWnHoXMb6eXWmYKMJrAoveLa+2cFm1Agf
\n7nLhA4R4lqm9IpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAJkD4wHW54Pwd4Ctfk9o
\njHjWB7pQlUYpTZO9dm+4fpCMn9Okf43AE2yAOaAP94GdzdDJkxfciXKcsYr9IIuk
\nfaoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BUlGKMWXzuEd
\n3fy+1rCUwzOp9LSjtJYf4ege
\n-----END PRIVATE KEY-----",
"type": "server",
"update_time": "2017-02-25 09:38:27"
}

Status Code

For details, see **Status Codes**.

10.1.9.5 Deleting a Certificate

Function

This API is used to delete a specific certificate.

Constraints

If the target certificate is used by a listener, the certificate cannot be deleted, and 409 code will be displayed.

URI

DELETE /v2.0/lbaas/certificates/{certificate_id}

Table 10-207 Parameter description

Parameter	Mandatory	Type	Description
certificate_id	Yes	String	Specifies the certificate ID.

Request

- Request parameters

  None

Response

- Response parameters

  None

Example Request

- Example request: Deleting a certificate

```
DELETE https://{Endpoint}/v2.0/lbaas/certificates/23ef9aad4ecb463580476d324a6c71af
```

Example Response

- Example response 1

  None

Status Code

For details, see **Status Codes**.

10.2 Asynchronous Job Query (Discarded)

Function

This API is used to query the execution status of an asynchronous job.

URI

GET /v1.0/{project_id}/jobs/{job_id}

Table 10-208 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID.

Parameter	Mandatory	Type	Description
job_id	Yes	String	Specifies the unique ID assigned to the job for querying the execution status in Combined API.

Request

None

Response

Table 10-209 Response parameters

Parameter	Type	Description
status	String	Specifies the job execution status. **SUCCESS**: The job was successfully executed. **FAIL**: The job failed. **RUNNING**: The job is in progress. **INIT**: The job is being initialized.
entities	*Dictionary data structure*	Specifies the resource information or error information. The ELB resource ID is used as an example in the response example.
job_id	String	Specifies the unique ID assigned to the job for querying the execution status in Combined API.
job_type	String	Specifies the job type.
error_code	String	Specifies the error code.
fail_reason	String	Specifies the cause of an error.

Example

- Example request

  None

- Example response

```
{
    "status": "RUNNING",
    "entities":
    {"elb_id": "ea3e5715b68850a747ec41f335625c08"},
    "job_id": "4010b39b4fd3d5ff014fd943bac41619",
```



```
    "job_type": "deleteELB",
    "begin_time": "2015-09-17T03:05:38.756Z",
    "end_time": "",
    "error_code":null,
    "fail_reason":null
}
```

Status Code

- Normal

  200

- Error

Status Code	Description
400 badRequest	Request error.
401 unauthorized	Authentication failed.
403 userDisabled	You do not have the permission to perform the operation.
404 Not Found	The requested page does not exist.
500 authFault	System error.
503 serviceUnavailable	The service is unavailable.

10.3 Querying Versions (Discarded)

Function

Queries all available versions.

If there is no version added to the URL, all available versions are returned.

URI

GET /

Request

None

Response

None

Example

- Example request

```
GET /
```

- Example response

```
{
  "versions": [
    {
       "status": "CURRENT",
       "id": "v2.0",
       "links": [
       {
          "href": "http://192.168.82.231:9696/v2.0",
          "rel": "self"
       }
      ]
     }
   ]
}
```

10.4 Getting Started

10.4.1 Creating a Load Balancer

Scenarios

Assume that you have created a VPC and several ECSs on the cloud platform. To ensure high performance and availability of ECSs, a load balancer is required to distribute requests to different backend ECSs.

This section describes how to invoke the API to create a load balancer.

NOTE

The validity period of a token obtained from IAM is 24 hours. If you want to use a token for authentication, cache it to avoid frequently calling the IAM API.

Involved APIs

If you use a token for authentication, you must obtain the token and add **X-Auth-Token** to the request header of the ELB API when making an API call.

- IAM API used to obtain the token
- ELB API used to create a load balancer

Procedure

1. Obtain the token by referring to **Authentication**.
2. Send **POST https://ELB endpoint/v2.0/lbaas/loadbalancers**.
3. Add **X-Auth-Token** to the request header.
4. Specify the following parameters in the request body:

```
{
   "loadbalancer": {
      "name": "loadbalancer1", //Load balancer name
      "description": "simple lb", //Load balancer description
      "vip_subnet_id": "58077bdb-d470-424b-8c45-2e3c65060a5b", //ID of the IPv4 subnet where the load balancer works
      "vip_address": "10.0.0.4" //IP address of the load balancer
   }
}
```

If the request is successful, the response body is returned.

If the request fails, an error code and error information are returned. For details, see **Status Codes**.

10.4.2 Obtaining a Token

Application Scenarios

If you use a token for authentication, you must obtain the token and add **X-Auth-Token** to the request header of the API when making a call.

Authenticating the Token

Step 1 Send **POST https://***IAM endpoint***/v3/auth/tokens**. Obtain the Identity and Access Management (IAM) endpoint and region name in the message body.

See **Regions and Endpoints**.

The following is an example request:

NOTE

The italic words in the following example need to be replaced with the actual values. For details, see **Obtaining a User Token**.

```
{
  "auth": {
    "identity": {
      "methods": [
        "password"
      ],
      "password": {
        "user": {
          "name": "username",
          "password": "password",
          "domain": {
            "name": "domainname"
          }
        }
      }
    },
    "scope": {
      "project": {
        "name": "aaa"
      }
    }
  }
}
```

Step 2 Obtain the token. The token is the value of **X-Subject-Token** in the response.

Step 3 Call a service API, add **X-Auth-Token** to the request header, and set the value of **X-Auth-Token** to the token obtained in **Step 2**.

----End

10.4.3 Creating a Load Balancer

Assume that you have created a Virtual Private Cloud (VPC) and several Elastic Cloud Servers (ECSs) on the cloud platform. To ensure high performance and availability of ECSs, a load balancer is required to distribute requests to different backend ECSs.

API Format

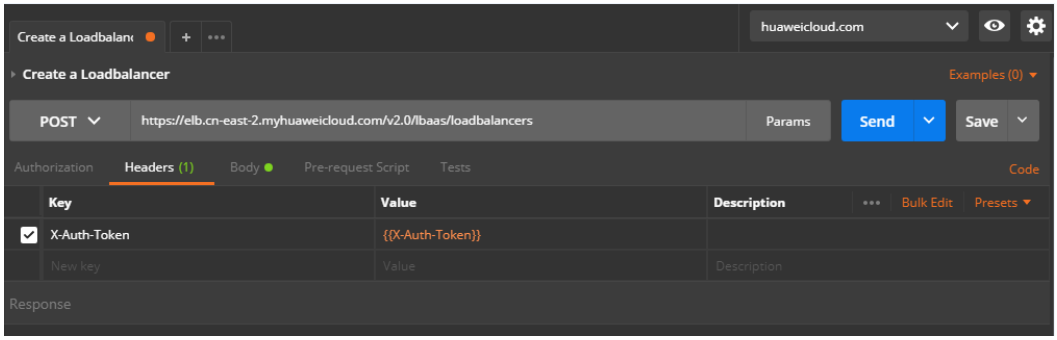
Method	URI	Description
POST	/v2.0/lbaas/loadbalancers	Creates a load balancer.

Procedure

Step 1 Set the request header.

Set the header in Postman and place the obtained token in the header.

Figure 10-1 Request header

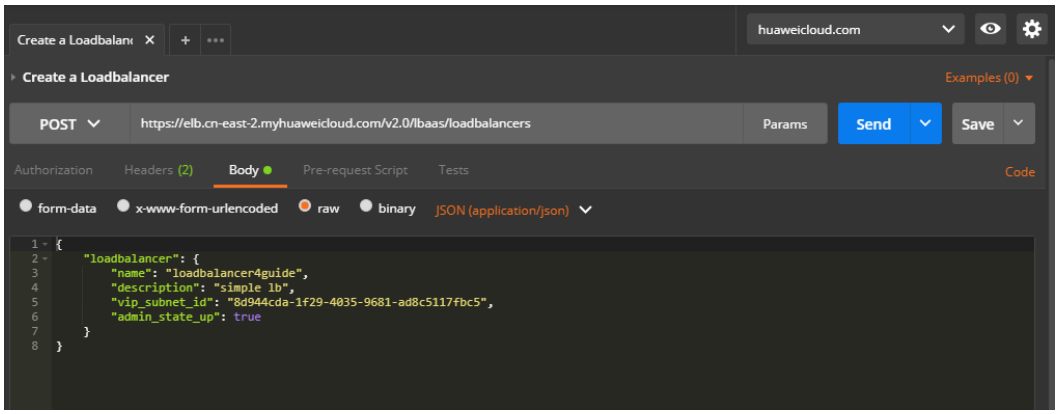


NOTE

The value of the token can be transferred through an environment variable or directly entered.

Step 2 Under **Body**, set the request body.

Figure 10-2 Request body



You can refer to **Sample Code** to set the request body, or add other required fields by referring to the Elastic Load Balance API Reference.

Step 3 Enter the URL.

The request URL consists of the following parts:

Endpoint				URI
https://	elb	.cn-north-1	.myhuaweicloud.com	/v2.0/lbaas/loadbalancers
-	Service name	Region	Endpoint	URI

Step 4 Send the request. Set the POST request method and click **Send** to wait for response from the server.

```
{
   "loadbalancer": {
      "description": "simple lb",
      "admin_state_up": true,
      "tenant_id": "0d0bf0e8fb564cc9abbe526dbdca9248",
      "provisioning_status": "ACTIVE",
      "vip_subnet_id": "8d944cda-1f29-4035-9681-ad8c5117fbc5",
      "listeners": [],
      "vip_address": "192.168.0.144",
      "vip_port_id": "b06bdc8f-cc00-41b4-8aba-280a333342ee",
      "provider": "vlb",
      "pools": [],
      "id": "bb2f1569-4c03-4e48-8e02-a2d831c0db56",
      "operating_status": "ONLINE",
      "name": "loadbalancer4guide"
   }
}
```

If the request is correct, information about the newly created load balancer is displayed. After logging in to the web console, you can see a load balancer named **loadbalancer4guide**.

----End

Sample Code

Request body in **Step 2**

```
{
   "loadbalancer": {
      "name": "loadbalancer1",
      "description": "simple lb",
      "vip_subnet_id": "58077bdb-d470-424b-8c45-2e3c65060a5b",
      "admin_state_up": true
   }
}
```

NOTE

The value of **vip_subnet_id** is the ID of the subnet where the create load balancer works.

10.4.4 Creating a Public Network Load Balancer

When an EIP is bound to a private network load balancer, the load balancer becomes a public network load balancer. Clients can access backend servers through this load balancer over Internet.

Apply for an EIP

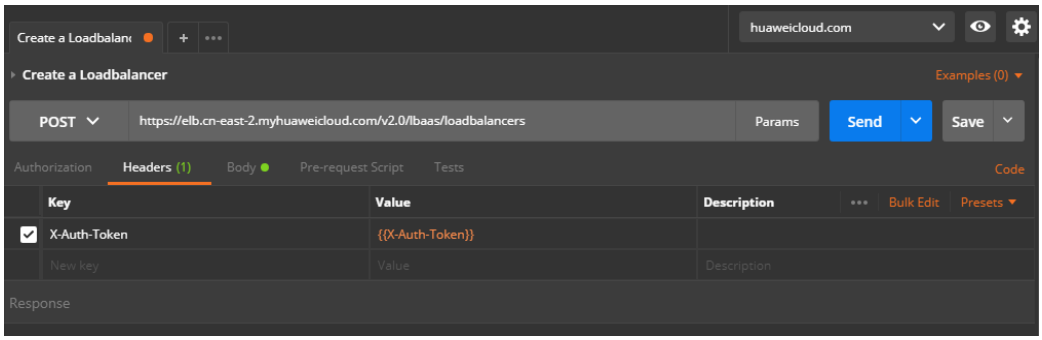
API Format

Method	URI	Description
POST	/v1/{tenant_id}/publicips	Applies for an EIP.

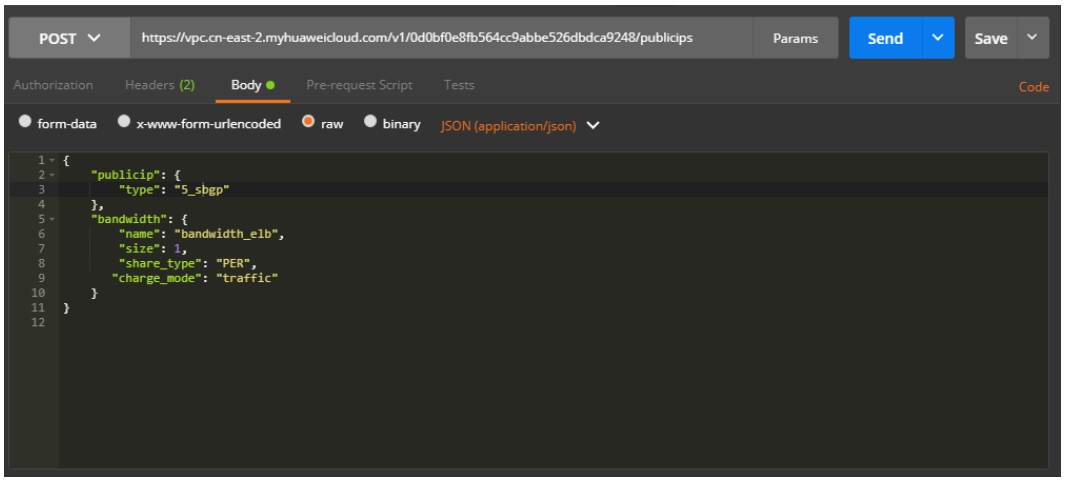
Procedure

Step 1 Set the request header.

Set the header in Postman and place the obtained token in the header.



Step 2 Under **Body**, set the request body.



Step 3 Enter the URL.

```
https://vpc.cn-east-2.myhuaweicloud.com/v1/0d0bf0e8fb564cc9abbe526dbdca9248/publicips
```

Step 4 Send the request. Set the POST request method and click **Send** to wait for response from the server.

```
{
   "publicip": {
      "id": "73c079fc-357a-4d34-8ba1-818a9d9a2aa2",
      "status": "PENDING_CREATE",
      "type": "5_sbgp",
      "public_ip_address": "122.112.235.121",
      "tenant_id": "0d0bf0e8fb564cc9abbe526dbdca9248",
      "create_time": "2018-07-11 02:40:32",
      "bandwidth_size": 0,
      "enterprise_project_id": "0"
   }
}
```


NOTE

Note that the value of **tenant_id** in the response body is the project ID on the web console.

----End

Sample Code

Request body in **Step 2**

```
{
   "publicip": {
      "type": "5_sbgp"
   },
   "bandwidth": {
      "name": "bandwidth_elb",
      "size": 1,
      "share_type": "PER",
      "charge_mode": "traffic"
   }
}
```

NOTE

For details about fields in the request body and their formats, see the *Virtual Private Cloud API Reference*.

Bind the EIP

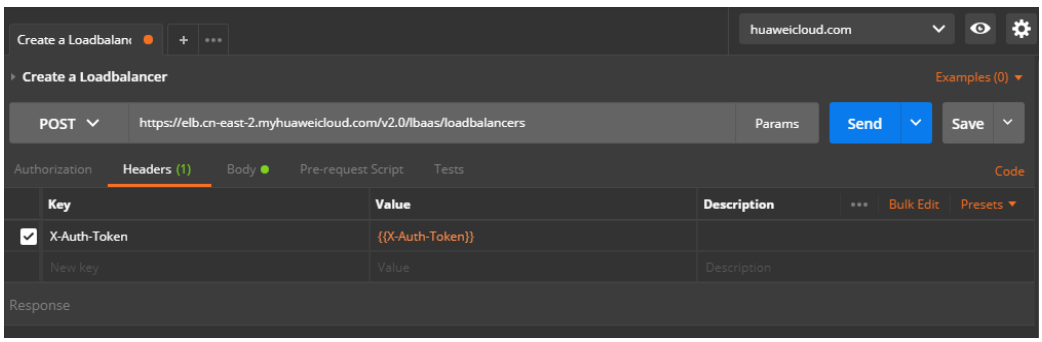
API Format

Method	URI	Description
PUT	/v1/{tenant_id}/publicips/{publicip_id}	Binds the EIP to a load balancer.

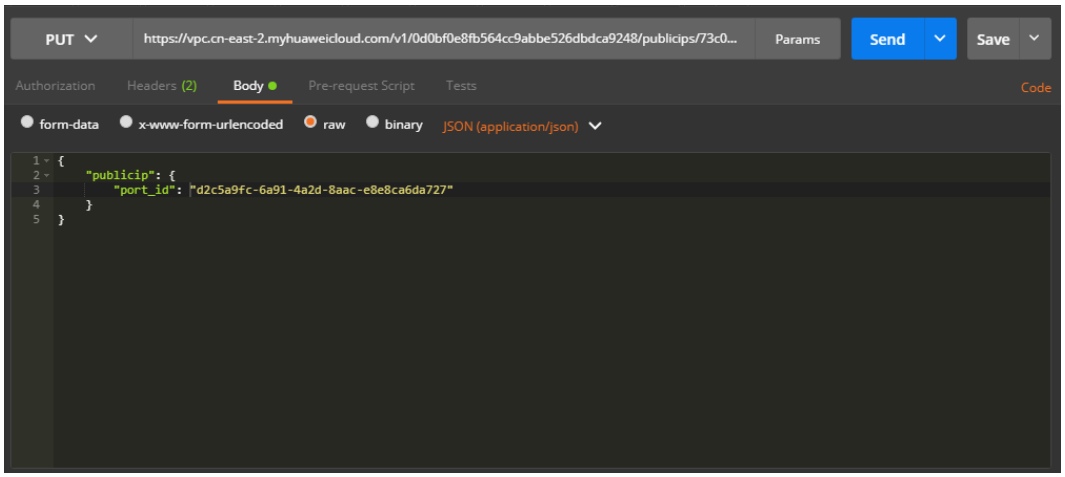
Procedure

Step 1 Set the request header.

Set the header in Postman and place the obtained token in the header.



Step 2 Under **Body**, set the request body.



NOTE

The value of **port_id** can be obtained by calling the VPC API. The request is as follows:

```
GET https://vpc.cn-north-1.myhuaweicloud.com/v2.0/ports?network_id=Network ID&fixed_ips=ip_address=Private IP address of the load balancer
```

Choose **Network** > **Virtual Private Cloud**, click the target VPC name, and obtain the network ID and private IP address of the load balancer on the subnet details page.

Step 3 Enter the URL.

```
https://vpc.cn-east-2.myhuaweicloud.com/v1/{{project_id}}/publicips/{{eip_id}}
```

NOTE

eip_id is the ID returned when the EIP is assigned in **Apply for an EIP**.

Step 4 Send the request. Set the PUT request method and click **Send** to wait for response from the server.

```
{
    "publicip": {
        "id": "73c079fc-357a-4d34-8ba1-818a9d9a2aa2",
        "status": "ACTIVE",
        "type": "5_sbgp",
        "port_id": "d2c5a9fc-6a91-4a2d-8aac-e8e8ca6da727",
        "public_ip_address": "122.112.235.121",
        "private_ip_address": "192.168.0.160",
        "tenant_id": "0d0bf0e8fb564cc9abbe526dbdca9248",
        "create_time": "2018-07-11 02:40:32",
        "bandwidth_size": 1
    }
}
```

----End

Sample Code

Request body in **Step 2**

```
{
    "publicip": {
        "port_id": "d2c5a9fc-6a91-4a2d-8aac-e8e8ca6da727"
    }
}
```


10.4.5 Adding a Listener

API Format

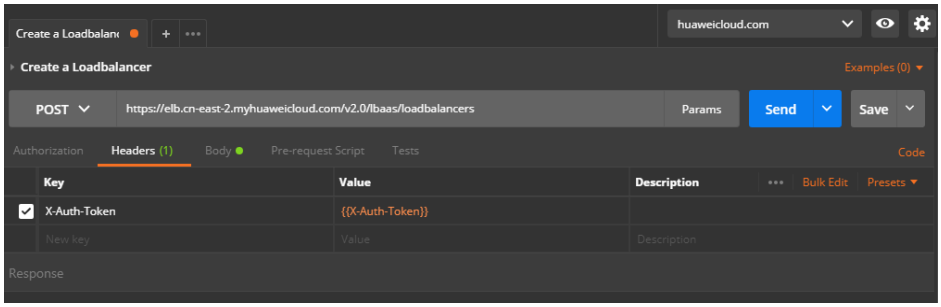
Method	URI	Description
POST	/v2.0/lbaas/listeners	Adds a listener.

Constraints

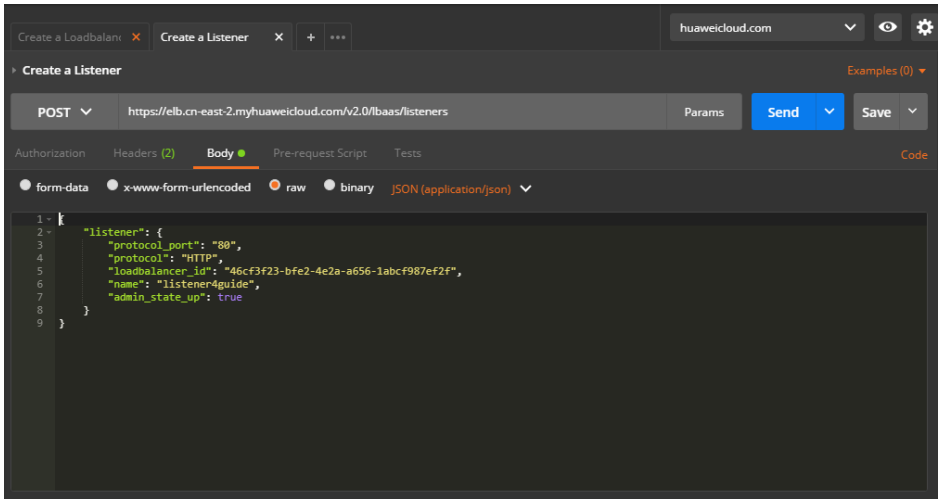
Each listener added a load balancer can listen on only one port.

Procedure

Step 1 Set the request header. Set the header in Postman and place the obtained token in the header.



Step 2 Under **Body**, set the request body.



Step 3 Enter the URL.

```
https://elb.cn-east-2.myhuaweicloud.com/v2.0/lbaas/listeners
```

Step 4 Send the request. Set the POST request method and click **Send** to wait for response from the server.

```
{
    "listener": {
        "protocol_port": 80,
```



```
    "protocol": "HTTP",
    "description": "",
    "default_tls_container_ref": null,
    "admin_state_up": true,
    "loadbalancers": [
       {
          "id": "abe3ee34-1882-408f-a2ba-1ce7e428d6e3"
       }
    ],
    "tenant_id": "0d0bf0e8fb564cc9abbe526dbdca9248",
    "sni_container_refs": [],
    "connection_limit": -1,
    "default_pool_id": null,
    "id": "779d77c8-f3f9-486d-a598-18e2aa2aa319",
    "name": "listener4guide"
  }
}
```


----End

Sample Code

Request body in **Step 2**


```
{
  "listener": {
    "protocol_port": "80",
    "protocol": "HTTP",
    "loadbalancer_id": "abe3ee34-1882-408f-a2ba-1ce7e428d6e3",
    "name": "listener4guide",
    "admin_state_up": true
  }
}
```

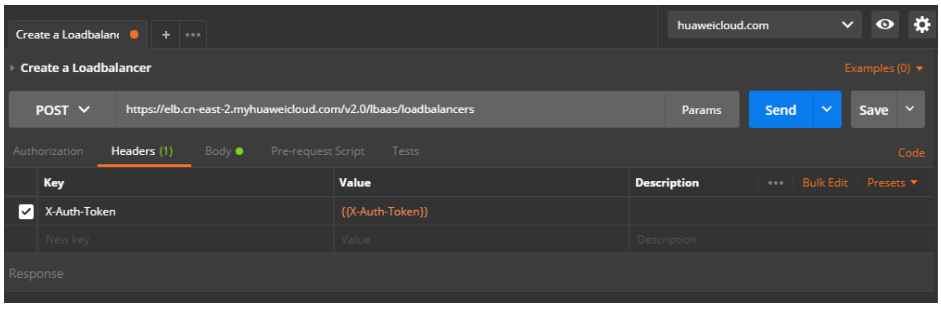

10.4.6 Creating a Backend Server Group

API Format

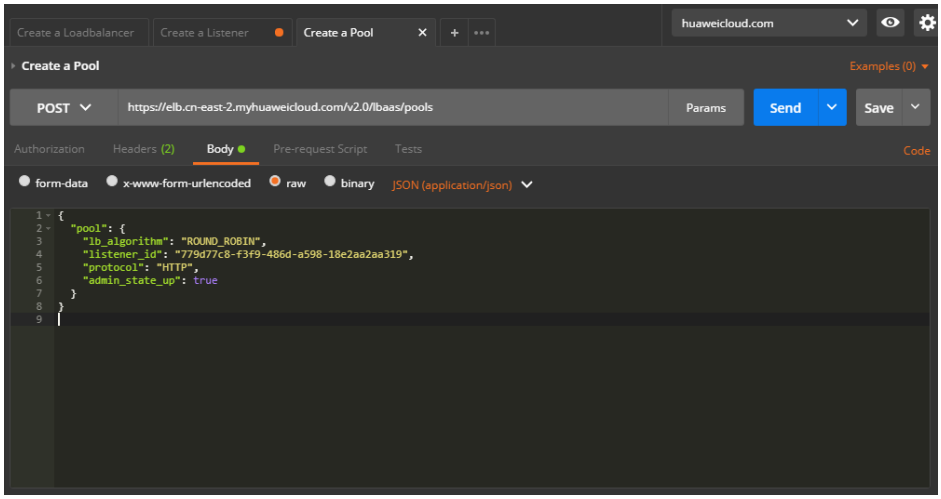
Method	URI	Description
POST	/v2.0/lbaas/pools	Adds a backend server group.

Procedure

Step 1 Set the request header. Set the header in Postman and place the obtained token in the header.



Step 2 Under **Body**, set the request body.



Step 3 Enter the URL.

```
https://elb.cn-east-2.myhuaweicloud.com/v2.0/lbaas/pools
```

Step 4 Send the request. Set the POST request method and click **Send** to wait for response from the server.

```
{
    "pool": {
        "lb_algorithm": "ROUND_ROBIN",
        "protocol": "HTTP",
        "description": "",
        "admin_state_up": true,
        "loadbalancers": [
            {
                "id": "abe3ee34-1882-408f-a2ba-1ce7e428d6e3"
            }
        ],
        "tenant_id": "0d0bf0e8fb564cc9abbe526dbdca9248",
        "session_persistence": null,
        "healthmonitor_id": null,
        "listeners": [
            {
                "id": "ecb4d58e-3b09-4a9d-9ad2-159b21e13f83"
            }
        ],
        "members": [],
        "id": "752c3773-a046-4966-a5d6-0ad7f9a49d0a",
        "name": ""
    }
}
```

----End

Sample Code

Request body in **Step 2**

```
{
    "pool": {
        "lb_algorithm": "ROUND_ROBIN",
        "listener_id": "{{listener_id}}",
        "protocol": "HTTP",
        "admin_state_up": true
    }
}
```


10.4.7 Adding Backend Servers

API Format

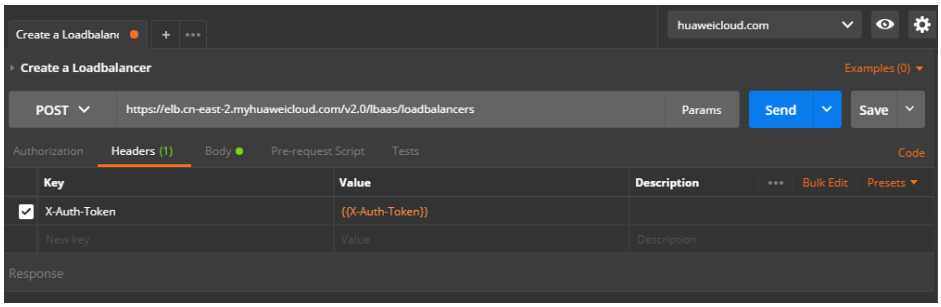
Method	URI	Description
POST	/v2.0/lbaas/pools/{pool_id}/members	Adds backend servers that belong to a backend server group.

Constraints

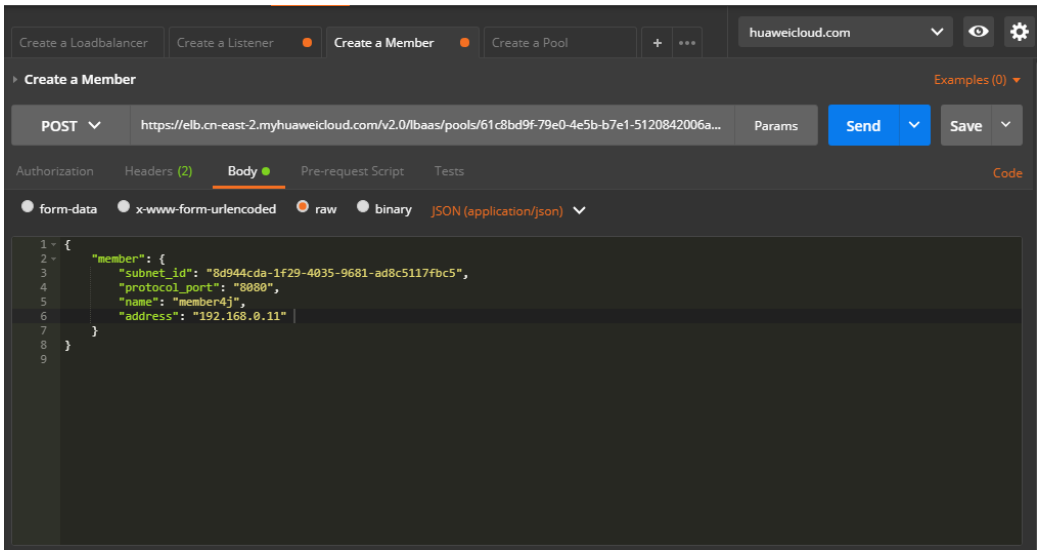
- Two backend servers in the same backend server group must have different IP addresses and ports.
- The subnet specified during server creation and the subnet to which the virtual IP address belongs must be in the same VPC.
- The value of **admin_state_up** must be **true**.

Procedure

Step 1 Set the request header. Set the header in Postman and place the obtained token in the header.



Step 2 Under **Body**, set the request body.



Step 3 Query the subnet ID and primary NIC IP address of the VM.

The URL is as follows:

```
GET https://{VPCEndpoint}/v2.0/ports?device_id={ecs_id}
```

Obtain the values of **subnet_id** and **ip_address** of the port for which **primary_interface** is **true** from the response body. The following is an example of the response body:

```
{
   "ports": [
      {
         "id": "4813697b-62ba-4f4b-90e5-13bbbdec7198",
         "name": "",
         "status": "ACTIVE",
         "admin_state_up": true,
         "fixed_ips": [
            {
               "subnet_id": "d97b6b89-6aa2-4636-a86b-132eb4eb566e",
               "ip_address": "10.1.1.89"
            }
         ],
         "mac_address": "fa:16:3e:cb:8d:0a",
         "network_id": "1b76b9c2-9b7e-4ced-81bd-d13f7389d7c9",
         "tenant_id": "04dd36f978800fe22f9bc00bea090736",
         "project_id": "04dd36f978800fe22f9bc00bea090736",
         "device_id": "f738c464-b5c2-45df-86c0-7f436620cd54",
         "device_owner": "compute:cn-north-4a",
         "security_groups": [
            "7a233393-5be2-4dff-8360-1558dd950f6e"
         ],
         "extra_dhcp_opts": [],
         "allowed_address_pairs": [],
         "binding:vnic_type": "normal",
         "binding:vif_details": {},
         "binding:profile": {},
         "port_security_enabled": true,
         "created_at": "2019-11-19T09:28:38",
         "updated_at": "2019-11-19T09:28:39"
      },
      {
         "id": "94971c39-46f0-443a-85e8-31cb7497c78e",
         "name": "",
         "status": "ACTIVE",
         "admin_state_up": true,
         "fixed_ips": [
            {
               "subnet_id": "8d944cda-1f29-4035-9681-ad8c5117fbc5",
               "ip_address": "192.168.0.11"
            }
         ],
         "mac_address": "fa:16:3e:5c:d2:57",
         "network_id": "1b76b9c2-9b7e-4ced-81bd-d13f7389d7c9",
         "tenant_id": "04dd36f978800fe22f9bc00bea090736",
         "project_id": "04dd36f978800fe22f9bc00bea090736",
         "device_id": "f738c464-b5c2-45df-86c0-7f436620cd54",
         "device_owner": "compute:cn-north-4a",
         "security_groups": [
            "a10dfc31-0055-4b84-b36e-1291b918125c",
            "7a233393-5be2-4dff-8360-1558dd950f6e"
         ],
         "extra_dhcp_opts": [],
         "allowed_address_pairs": [],
         "binding:vnic_type": "normal",
         "binding:vif_details": {
            "primary_interface": true
         },
         "binding:profile": {},
```



```
            "port_security_enabled": true,
            "created_at": "2019-11-12T17:17:51",
            "updated_at": "2019-11-12T17:17:51"
        }
    ]
}
```


Step 4 Enter the URL.

```
https://{ELBEndpoint}/v2.0/lbaas/pools/{pool_id}/members
```

Step 5 Send the request. Set the values of **subnet_id** and **ip_address** to these obtained in **Step 3**, select POST as the request method, and click **Send**.


```
{
    "member": {
        "name": "member4j",
        "weight": 1,
        "admin_state_up": false,
        "subnet_id": "8d944cda-1f29-4035-9681-ad8c5117fbc5",
        "tenant_id": "0d0bf0e8fb564cc9abbe526dbdca9248",
        "address": "192.168.0.11",
        "protocol_port": 8080,
        "id": "97f18d73-e97d-434c-8cb7-3274a83dda73",
        "operating_status": "ONLINE"
    }
}
```


----End

Sample Code

Request body in **Step 2**


```
{
    "member": {
        "subnet_id": "8d944cda-1f29-4035-9681-ad8c5117fbc5",
        "protocol_port": "8080",
        "name": "member4j",
        "address": "192.168.0.11"
    }
}
```


10.4.8 Configuring a Health Check

API Format

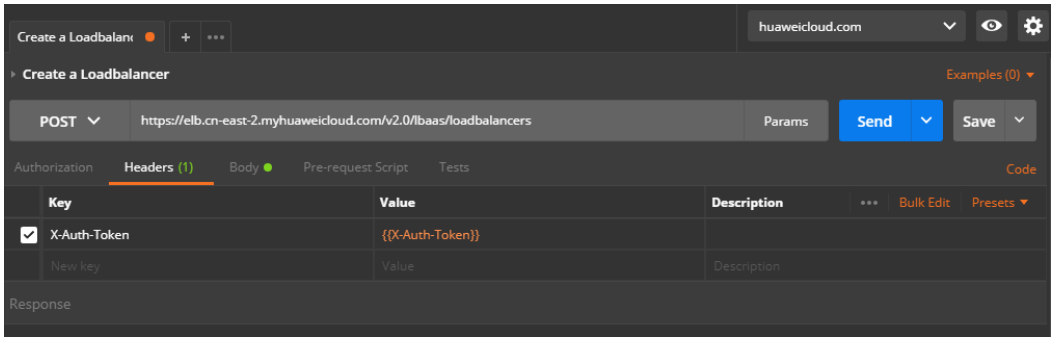
Method	URI	Description
POST	/v2.0/lbaas/healthmonitors	Configures a health check.

Constraints

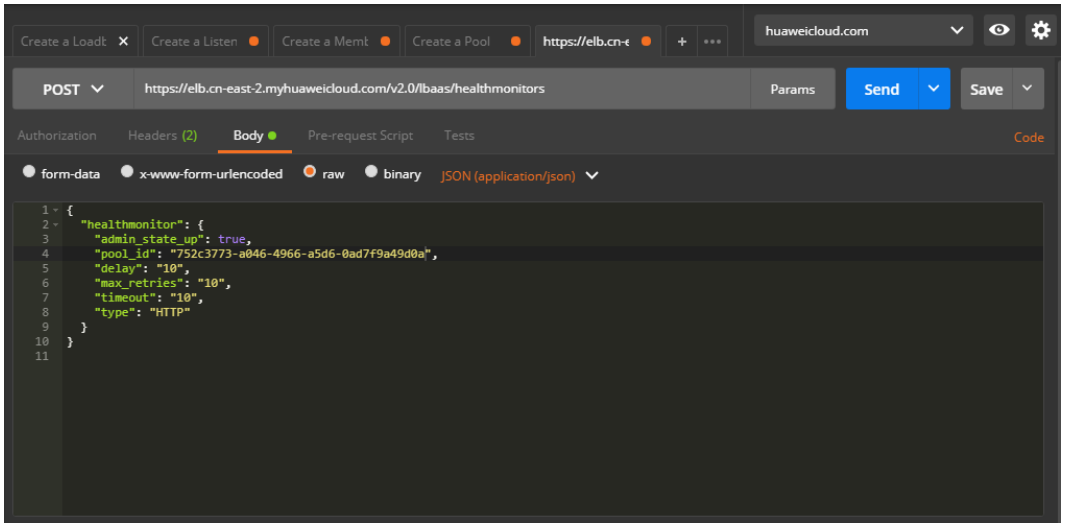
- The security group must have rules to allow access from the 100.125.0.0/16 network segment.
- The value of **admin_state_up** must be **true**.
- To use UDP for health checks, the backend server group must use UDP as backend protocol.

Procedure

Step 1 Set the request header. Set the header in Postman and place the obtained token in the header.



Step 2 Under **Body**, set the request body.



Step 3 Enter the URL.

```
https://elb.cn-east-2.myhuaweicloud.com/v2.0/lbaas/healthmonitors
```

Step 4 Send the request. Set the POST request method and click **Send** to wait for response from the server.

```
{
   "healthmonitor": {
      "monitor_port": null,
      "name": "",
      "admin_state_up": true,
      "tenant_id": "0d0bf0e8fb564cc9abbe526dbdca9248",
      "delay": 10,
      "expected_codes": "200",
      "max_retries": 10,
      "http_method": "GET",
      "timeout": 10,
      "pools": [
         {
            "id": "752c3773-a046-4966-a5d6-0ad7f9a49d0a"
         }
      ],
      "url_path": "/",
      "type": "HTTP",
```



```
        "id": "9b6d7438-a6eb-4d49-ae77-3c130e3b7ae8"
    }
}
```

----End

Sample Code

Request body in **Step 2**

```
{
  "healthmonitor": {
    "admin_state_up": true,
    "pool_id": "752c3773-a046-4966-a5d6-0ad7f9a49d0a",
    "delay": "10",
    "max_retries": "10",
    "timeout": "10",
    "type": "HTTP"
  }
}
```

10.4.9 Adding a Forwarding Policy

API Format

Method	URI	Description
POST	/v2.0/lbaas/l7policies	Adds a forwarding policy.

Application Scenarios

By adding forwarding policies and rules, you can forward different requests to a specific backend server.

Suppose that you have several servers on the cloud platform to provide services for the Internet, and the resources mainly include music (/music/{music_id}), images (/pic/{pic_id}), and files (/file/{file_id}). If there are no forwarding policies, each backend server has a copy of all resources. Requests from a client are always distributed to only one backend server. Therefore, only one copy is used. The storage cost increases as there are more and more backend servers.

Forwarding policies and rules provided by ELB can well solve this problem. In this way, the storage cost is reduced and you can obtain better economic benefits.

Constraints

- Forwarding policies can be added for listeners when **protocol** is set to **HTTP** or **TERMINATED_HTTPS**.
- The value of **redirect_pool** configured for the forwarding policy cannot be the same as that of **default_pool** configured for the listener.
- The backend server group specified in **redirect_pool** cannot be used by forwarding policies of other listeners.

Scenario Assumption

Assume that you have created a load balancer named **loadbalancer_1**. You can add a listener named **listener_1** and three backend server groups **pool_1**, **pool_2**, and **pool_3**. **pool_1** is the default backend server group of **listener_1**, and **pool_2** and **pool_3** are associated with **loadbalancer_1**. For better load distribution, HTTP requests whose URI starts with **/music** are sent to **pool_2**, and HTTP requests whose URI starts with **/pic** are forwarded to **pool_3**.

Procedure

To match the URIs, HTTP messages need to be parsed. Therefore, the listener and three backend server groups must use the HTTP or HTTPS protocol.

Step 1 Add an HTTP listener named **listener_1**.

```
POST https://elb.cn-east-2.myhuaweicloud.com/v2.0/lbaas/listeners
{
    "listener": {
        "protocol_port": "80",
        "protocol": "HTTP",
        "loadbalancer_id": "abe3ee34-1882-408f-a2ba-1ce7e428d6e3",
        "name": "listener_1",
        "admin_state_up": true
    }
}
```

Step 2 Add a backend server group named **pool_1** and its backend protocol is HTTP.

```
POST https://elb.cn-east-2.myhuaweicloud.com/v2.0/lbaas/pools/
{
  "pool": {
  "name":"pool_1",
    "lb_algorithm": "ROUND_ROBIN",
    "listener_id": "a7b996cf-23ec-4c0b-b310-45495d29f80c",
    "protocol": "HTTP",
    "admin_state_up": true
  }
}
```

Step 3 Add a backend server group named **pool_2** and its backend protocol is HTTP.

```
POST https://elb.cn-east-2.myhuaweicloud.com/v2.0/lbaas/pools/
{
  "pool": {
  "name":"pool_2",
    "lb_algorithm": "ROUND_ROBIN",
    "listener_id": "a7b996cf-23ec-4c0b-b310-45495d29f80c",
    "protocol": "HTTP",
    "admin_state_up": true
  }
}
```

Step 4 Add a backend server group named **pool_3** and its backend protocol is HTTP.

```
POST https://elb.cn-east-2.myhuaweicloud.com/v2.0/lbaas/pools/
{
  "pool": {
  "name":"pool_3",
    "lb_algorithm": "ROUND_ROBIN",
    "listener_id": "a7b996cf-23ec-4c0b-b310-45495d29f80c",
    "protocol": "HTTP",
    "admin_state_up": true
  }
}
```

Step 5 Add a forwarding policy to **pool_2**.


```
POST https://elb.cn-east-2.myhuaweicloud.com/v2.0/lbaas/l7policies
{
    "l7policy": {
        "action": "REDIRECT_TO_POOL",
        "listener_id": "a7b996cf-23ec-4c0b-b310-45495d29f80c",
        "redirect_pool_id": "b9a01911-8364-44d8-ab5a-4f635820edb2",
        "name": "l7policy_music",
        "admin_state_up": true
    }
}
```

Step 6 Add a forwarding policy to **pool_3**.

```
POST https://elb.cn-east-2.myhuaweicloud.com/v2.0/lbaas/l7policies
{
    "l7policy": {
        "action": "REDIRECT_TO_POOL",
        "listener_id": "a7b996cf-23ec-4c0b-b310-45495d29f80c",
        "redirect_pool_id": "3a9b8338-3086-4acc-92e6-83c5e750e44a",
        "name": "l7policy_pic",
        "admin_state_up": true
    }
}
```

Step 7 Check the created forwarding policies. They do not match any request because there are no specific forwarding rules. To make the forwarding policies to take effect, forwarding rules must be added to forward requests with different URIs.

----End

10.4.10 Adding a Forwarding Rule

API Format

Method	URI	Description
POST	/v2.0/lbaas/l7policies/{l7policy_id}/rules	Adds a forwarding rule.

Constraints

The type of forwarding rules for the same forwarding policy cannot be the same.

Procedure

Step 1 Set the request header. Set the header in Postman and place the obtained token in the header.

Step 2 Create a forwarding rule for the request whose name starts with **/music**.

```
POST https://elb.cn-east-2.myhuaweicloud.com/v2.0/lbaas/l7policies/5b94fb42-
b018-4ad6-9ba6-0e8a509c6821/rules
{
    "rule": {
        "compare_type": "STARTS_WITH",
        "type": "PATH",
        "value": "/music"
    }
}
```


Step 3 Create a forwarding rule for the request whose name starts with **/pic**.

```
POST https://elb.cn-east-2.myhuaweicloud.com/v2.0/lbaas/l7policies/
f6c5862d-460c-4ab6-8dc7-2294df442f67/rules
{
   "rule": {
      "compare_type": "STARTS_WITH",
      "type": "PATH",
      "value": "/pic"
   }
}
```

Step 4 Check the created forwarding rules on the web console.

----End

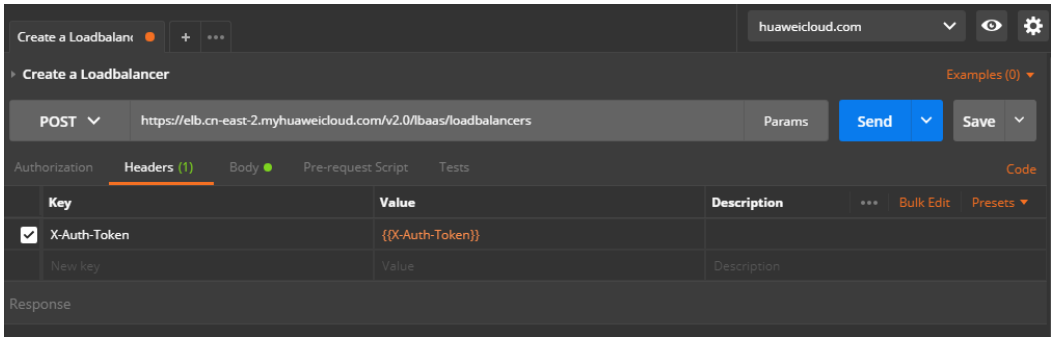
10.4.11 Adding a Whitelist

API Format

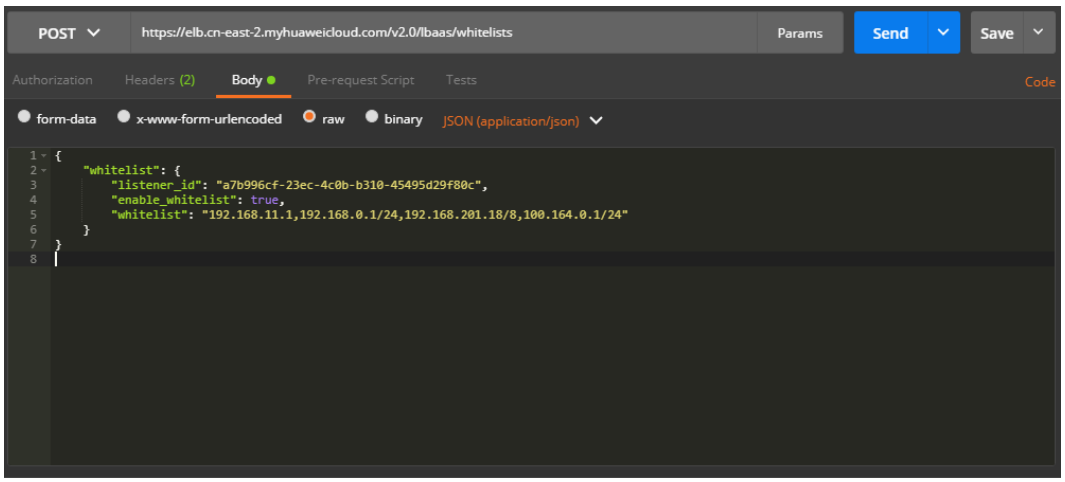
Method	URI	Description
POST	/v2.0/lbaas/whitelists	Adds a whitelist.

Procedure

Step 1 Set the request header. Set the header in Postman and place the obtained token in the header.



Step 2 Under **Body**, set the request body.



Step 3 Enter the URL.

```
https://elb.cn-east-2.myhuaweicloud.com/v2.0/lbaas/whitelists
```

Step 4 Send the request.

Set the POST request method and click **Send** to wait for response from the server.

```
{
    "whitelist": {
        "tenant_id": "0d0bf0e8fb564cc9abbe526dbdca9248",
        "whitelist": "192.168.11.1,192.168.0.1/24,192.168.201.18/8,100.164.0.1/24",
        "enable_whitelist": true,
        "id": "317a0ea1-e47b-4e8b-996f-0556270245c3",
        "listener_id": "a7b996cf-23ec-4c0b-b310-45495d29f80c"
    }
}
```

----End

Sample Code

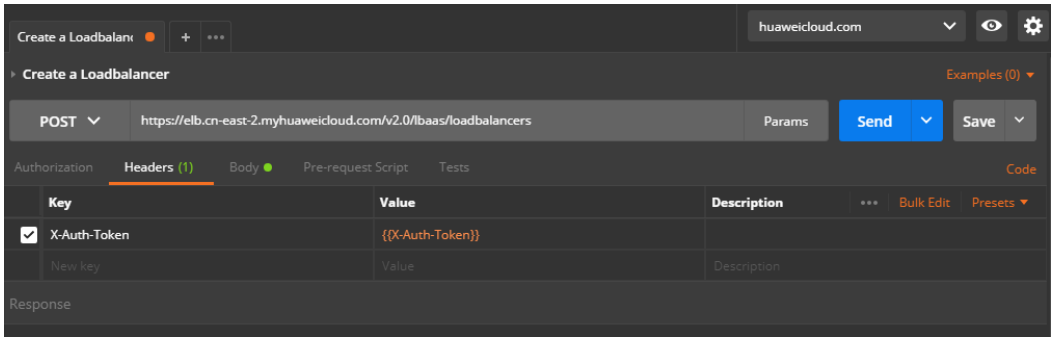
Request body in **Step 2**

```
{
    "whitelist": {
        "listener_id": "a7b996cf-23ec-4c0b-b310-45495d29f80c",
        "enable_whitelist": true,
        "whitelist": "192.168.11.1,192.168.0.1/24,192.168.201.18/8,100.164.0.1/24"
    }
}
```

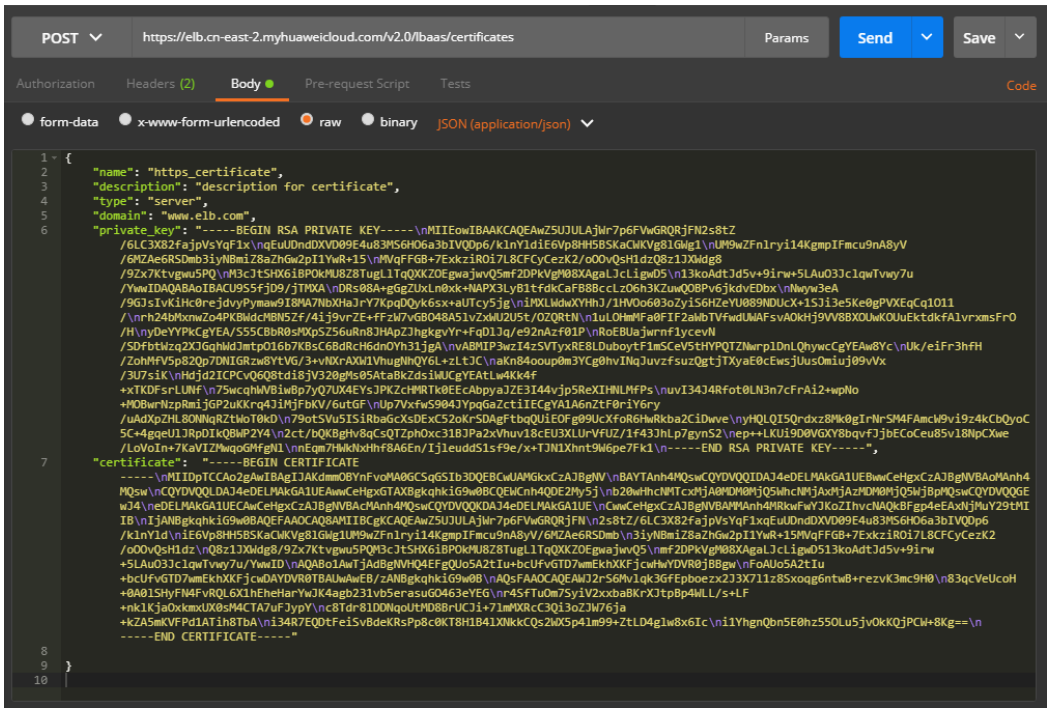
10.4.12 Creating an SSL Certificate

Step 1 Set the request header.

Set the header in Postman and place the obtained token in the header.



Step 2 Under **Body**, set the request body.



Step 3 Enter the URL.

```
https://elb.cn-east-2.myhuaweicloud.com/v2.0/lbaas/certificates
```

Step 4 Send the request. Set the POST request method and click **Send** to wait for response from the server.


```
{
    "update_time": "2018-07-11 02:10:05",
    "private_key": "-----BEGIN RSA PRIVATE KEY-----
\nMIIEowIBAAKCAQEAwZ5UJULAjWr7p6FVwGRQRjFN2s8tZ/6LC3X82fajpVsYqF1x
\nqEuUDndDXVD09E4u83MS6HO6a3bIVQDp6/
klnYldiE6Vp8HH5BSKaCWKVg8lGWg1\nUM9wZFnlryi14KgmpIFmcu9nA8yV/
6MZAe6RSDmb3iyNBmiZ8aZhGw2pI1YwR+15\nMVqFFGB+7ExkziROi7L8CFCyCezK2/
oOOvQsH1dzQ8z1JXWdg8/9Zx7Ktvgwu5PQ
\nM3cJtSHX6iBPOkMU8Z8TugLlTqQXKZOEgwajwvQ5mf2DPkVgM08XAgaLJcLigwD5\n13koAdtJd5v+9irw
+5LAuO3JclqwTvwy7u/YwwIDAQABAoIBACU9S5fjD9/jTMXA\nDRs08A+gGgZUxLn0xk
+NAPX3LyB1tfdkCaFB8BccLzO6h3KZuwQOBPv6jkdvEDbx\nNwyw3eA/
9GJsIvKiHc0rejdvyPymaw9I8MA7NbXHaJrY7KpqDQyk6sx+aUTcy5jg\niMXLWdwXYHhJ/
1HVOo603oZyiS6HZeYU089NDUcX+1SJi3e5Ke0gPVXEqCq1O11/\nrh24bMxnwZo4PKBWdcMBN5Zf/4ij9vrZE
+fFzW7vGBO48A5lvZxWU2U5t/OZQRtN
\n1uLOHmMFa0FIF2aWbTVfwdUWAFsvAOkHj9VV8BXOUwKOUuEktdkfAlvrxmsFrO/H\nyDeYYPkCgYEA/
S55CBbR0sMXpSZ56uRn8JHApZJhgkgvYr+FqDUq/e92nAzf01P\nRoEBUajwrnf1ycevN/
SDfbtWzq2XJGqhWdJmtpO16b7KBsC6BdRcH6dnOYh31jgA
\nvABMIP3wzI4zSVTyxRE8LDuboytF1mSCeV5tHYPQTZNwrplDnLQhywcCgYEAw8Yc\nUk/eiFr3hfH/
ZohMfV5p82Qp7DNIGRzw8YtVG/3+vNXrAXW1VhugNhQY6L+zLtJC
\naKn84ooup0m3YCg0hvINqJuvzfsuzQgtjTXyaE0cEwsjUusOmiuj09vVx/3U7siK
\nHdjd2ICPCvQ6Q8tdi8jV320gMs05AtaBkZdsiWUCgYEAtLw4Kk4f+xTKDFsrLUNf
\n75wcqhWVBiwBp7yQ7UX4EYsJPKZcHMRTk0EEcAbpyaJZE3I44vjp5ReXIHNLMfPs
\nuvI34J4Rfot0LN3n7cFrAi2+wpNo+MOBwrNzpRmijGP2uKKrq4JiMjFbKV/6utGF
\nUp7VxfwS904JYpqGaZctiIECgYA1A6nZtF0riY6ry/uAdXpZHL8ONNqRZtWoT0kD
\n79otSVu5ISiRbaGcXsDExC52oKrSDAgFtbqQUiEOFg09UcXfoR6HwRkba2CiDwve
\nyHQLQI5Qrdxz8Mk0gIrNrSM4FAmcW9vi9z4kCbQyoC5C+4gqeUlRpDIkQBWP2Y4\n2ct/
bQKBgHv8qCsQTZphOxc31BJPa2xVhuv18cEU3XLUrVfUZ/1f43JhLp7gynS2\nep+
+LKUi9D0VGXY8bqvfJjbECoCeu85vl8NpCXwe/LoVoIn+7KaVIZMwqoGMfgNl\nnEqm7HWkNxHhf8A6En/
IjleuddS1sf9e/x+TJN1Xhnt9W6pe7Fk1\n-----END RSA PRIVATE KEY-----",
    "id": "e3c066329baa4a90bfebe13ec3d3cb8c",
    "name": "https_certificate",
    "domain": "www.elb.com",
    "description": "description for certificate",
    "tenant_id": "0d0bf0e8fb564cc9abbe526dbdca9248",
    "create_time": "2018-07-11 02:10:05",
```



```
    "certificate": "-----BEGIN CERTIFICATE-----
\nMIIDpTCCAo2gAwIBAgIJAKdmmOBYnFvoMA0GCSqGSIb3DQEBCwUAMGkxCzAJBgNV
\nBAYTAnh4MQswCQYDVQQIDAJ4eDELMAkGA1UEBwwCeHgxCzAJBgNVBAoMAnh4MQsw
\nCQYDVQQLDAJ4eDELMAkGA1UEAwwCeHgxGTAXBgkqhkiG9w0BCQEWCnh4QDE2My5j
\nb20wHhcNMTcxMjA0MDM0MjQ5WhcNMjAxMjAzMDM0MjQ5WjBpMQswCQYDVQQGEwJ4\neDELMAkGA
1UECAwCeHgxCzAJBgNVBAcMAnh4MQswCQYDVQQKDAJ4eDELMAkGA1UE
\nCwwCeHgxCzAJBgNVBAMMAnh4MRkwFwYJKoZIhvcNAQkBFgp4eEAxNjMuY29tMIIB
\nIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwZ5UJULAjWr7p6FVwGRQRjFN\n2s8tZ/
6LC3X82fajpVsYqF1xqEuUDndDXVD09E4u83MS6HO6a3bIVQDp6/klnYld
\niE6Vp8HH5BSKaCWKVg8lGWg1UM9wZFnlryi14KgmpIFmcu9nA8yV/6MZAe6RSDmb
\n3iyNBmiZ8aZhGw2pI1YwR+15MVqFFGB+7ExkziROi7L8CFCyCezK2/oOOvQsH1dz
\nQ8z1JXWdg8/9Zx7Ktvgwu5PQM3cJtSHX6iBPOkMU8Z8TugLlTqQXKZOEgwajwvQ5\nmf2DPkVgM08XAgaLJ
cLigwD513koAdtJd5v+9irw+5LAuO3JclqwTvwy7u/YwwID\nAQABo1AwTjAdBgNVHQ4EFgQUo5A2tIu
+bcUfvGTD7wmEkhXKFjcwHwYDVR0jBBgw\nFoAUo5A2tIu
+bcUfvGTD7wmEkhXKFjcwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0B
\nAQsFAAOCAQEAWJ2rS6Mvlqk3GfEpboezx2J3X7l1z8Sxoqg6ntwB+rezvK3mc9H0\n83qcVeUcoH
+0A0lSHyFN4FvRQL6X1hEheHarYwJK4agb231vb5erasuGO463eYEG\nr4SfTuOm7SyiV2xxbaBKrXJtpBp4WLL/s
+LF+nklKjaOxkmxUX0sM4CTA7uFJypY\nc8Tdr8lDDNqoUtMD8BrUCJi+7lmMXRcC3Qi3oZJW76ja
+kZA5mKVFPd1ATih8TbA\ni34R7EQDtFeiSvBdeKRsPp8c0KT8H1B4lXNkkCQs2WX5p4lm99+ZtLD4glw8x6Ic
\ni1YhgnQbn5E0hz55OLu5jvOkKQjPCW+8Kg==\n-----END CERTIFICATE-----",
    "type": "server"
}
```


----End

Sample Code

Request body in **Step 2**


```
{
    "name": "https_certificate",
    "description": "description for certificate",
    "type": "server",
    "domain": "www.elb.com",
    "private_key": "-----BEGIN RSA PRIVATE KEY-----
\nMIIEowIBAAKCAQEAwZ5UJULAjWr7p6FVwGRQRjFN2s8tZ/6LC3X82fajpVsYqF1x
\nqEuUDndDXVD09E4u83MS6HO6a3bIVQDp6/
klnYldiE6Vp8HH5BSKaCWKVg8lGWg1\nUM9wZFnlryi14KgmpIFmcu9nA8yV/
6MZAe6RSDmb3iyNBmiZ8aZhGw2pI1YwR+15\nMVqFFGB+7ExkziROi7L8CFCyCezK2/
oOOvQsH1dzQ8z1JXWdg8/9Zx7Ktvgwu5PQ
\nM3cJtSHX6iBPOkMU8Z8TugLlTqQXKZOEgwajwvQ5mf2DPkVgM08XAgaLJcLigwD5\n13koAdtJd5v+9irw
+5LAuO3JclqwTvwy7u/YwwIDAQABAoIBACU9S5fjD9/jTMXA\nDRs08A+gGgZUxLn0xk
+NAPX3LyB1tfdkCaFB8BccLzO6h3KZuwQOBPv6jkdvEDbx\nNwyw3eA/
9GJsIvKiHc0rejdvyPymaw9I8MA7NbXHaJrY7KpqDQyk6sx+aUTcy5jg\niMXLWdwXYHhJ/
1HVOo603oZyiS6HZeYU089NDUcX+1SJi3e5Ke0gPVXEqCq1O11/\nrh24bMxnwZo4PKBWdcMBN5Zf/4ij9vrZE
+fFzW7vGBO48A5lvZxWU2U5t/OZQRtN
\n1uLOHmMFa0FIF2aWbTVfwdUWAFsvAOkHj9VV8BXOUwKOUuEktdkfAlvrxmsFrO/H\nyDeYYPkCgYEA/
S55CBbR0sMXpSZ56uRn8JHApZJhgkgvYr+FqDlJq/e92nAzf01P\nRoEBUajwrnf1ycevN/
SDfbtWzq2XJGqhWdJmtpO16b7KBsC6BdRcH6dnOYh31jgA
\nvABMIP3wzI4zSVTyxRE8LDuboytF1mSCeV5tHYPQTZNwrplDnLQhywcCgYEAw8Yc\nUk/eiFr3hfH/
ZohMfV5p82Qp7DNIGRzw8YtVG/3+vNXrAXW1VhugNhQY6L+zLtJC
\naKn84ooup0m3YCg0hvINqJuvzfsuzQgtjTXyaE0cEwsjUusOmiuj09vVx/3U7siK
\nHdjd2ICPCvQ6Q8tdi8jV320gMs05AtaBkZdsiWUCgYEAtLw4Kk4f+xTKDFsrLUNf
\n75wcqhWVBiwBp7yQ7UX4EYsJPKZcHMRTk0EEcAbpyaJZE3l44vjp5ReXIHNLMfPs
\nuvI34J4Rfot0LN3n7cFrAi2+wpNo+MOBwrNzpRmijGP2uKKrq4JiMjFbKV/6utGF
\nUp7VxfwS904JYpqGaZctiIECgYA1A6nZtF0riY6ry/uAdXpZHL8ONNqRZtWoT0kD
\n79otSVu5ISiRbaGcXsDExC52oKrSDAgFtbqQUiEOFg09UcXfoR6HwRkba2CiDwve
\nyHQLQI5Qrdxz8Mk0gIrNrSM4FAmcW9vi9z4kCbQyoC5C+4gqeUlRpDIkQBWP2Y4\n2ct/
bQKBgHv8qCsQTZphOxc31BJPa2xVhuv18cEU3XLUrVfUZ/1f43JhLp7gynS2\nep+
+LKUi9D0VGXY8bqvfJjbECoCeu85vl8NpCXwe/LoVoIn+7KaVIZMwqoGMfgNl\nnEqm7HWkNxHhf8A6En/
IjleuddS1sf9e/x+TJN1Xhnt9W6pe7Fk1\n-----END RSA PRIVATE KEY-----",
    "certificate": "-----BEGIN CERTIFICATE-----
\nMIIDpTCCAo2gAwIBAgIJAKdmmOBYnFvoMA0GCSqGSIb3DQEBCwUAMGkxCzAJBgNV
\nBAYTAnh4MQswCQYDVQQIDAJ4eDELMAkGA1UEBwwCeHgxCzAJBgNVBAoMAnh4MQsw
\nCQYDVQQLDAJ4eDELMAkGA1UEAwwCeHgxGTAXBgkqhkiG9w0BCQEWCnh4QDE2My5j
\nb20wHhcNMTcxMjA0MDM0MjQ5WhcNMjAxMjAzMDM0MjQ5WjBpMQswCQYDVQQGEwJ4\neDELMAkGA
1UECAwCeHgxCzAJBgNVBAcMAnh4MQswCQYDVQQKDAJ4eDELMAkGA1UE
\nCwwCeHgxCzAJBgNVBAMMAnh4MRkwFwYJKoZIhvcNAQkBFgp4eEAxNjMuY29tMIIB
\nIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwZ5UJULAjWr7p6FVwGRQRjFN\n2s8tZ/
```



```
6LC3X82fajpVsYqF1xqEuUDndDXVD09E4u83MS6HO6a3bIVQDp6/klnYld
\niE6Vp8HH5BSKaCWKVg8lGWg1UM9wZFnlryi14KgmpIFmcu9nA8yV/6MZAe6RSDmb
\n3iyNBmiZ8aZhGw2pI1YwR+15MVqFFGB+7ExkziROi7L8CFCyCezK2/oOOvQsH1dz
\nQ8z1JXWdg8/9Zx7Ktvgwu5PQM3cJtSHX6iBPOkMU8Z8TugLlTqQXKZOEgwajwvQ5\nmf2DPkVgM08XAgaLJ
cLigwD513koAdtJd5v+9irw+5LAuO3JclqwTvwy7u/YwwID\nAQABo1AwTjAdBgNVHQ4EFgQUo5A2tIu
+bcUfvGTD7wmEkhXKFjcwHwYDVR0jBBgw\nFoAUo5A2tIu
+bcUfvGTD7wmEkhXKFjcwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0B
\nAQsFAAOCAQEAWJ2rS6Mvlqk3GfEpboezx2J3X7l1z8Sxoqg6ntwB+rezvK3mc9H0\n83qcVeUcoH
+0A0lSHyFN4FvRQL6X1hEheHarYwJK4agb231vb5erasuGO463eYEG\nr4SfTuOm7SyiV2xxbaBKrXJtpBp4WLL/s
+LF+nklKjaOxkmxUX0sM4CTA7uFJypY\nc8Tdr8lDDNqoUtMD8BrUCJi+7lmMXRcC3Qi3oZJW76ja
+kZA5mKVFPd1ATih8TbA\ni34R7EQDtFeiSvBdeKRsPp8c0KT8H1B4lXNkkCQs2WX5p4lm99+ZtLD4glw8x6Ic
\ni1YhgnQbn5E0hz55OLu5jvOkKQjPCW+8Kg==\n-----END CERTIFICATE-----"
}
```

NOTE

To ensure information security for you and your customers, do not use the certificates and keys in the sample code.

A Appendix

A.1 Error Codes

If an error code starting with APIGW is returned after you call an API, rectify the fault by referring to the instructions provided in **API Gateway Error Codes**.

Status Code	Error Codes	Error Message	Description	Solution
400	ELB.0002	RequestBody is null or empty,request is invalid.	The request body is empty.	Configure the parameters by following the instructions in the Elastic Load Balance API Reference.
400	ELB.0004	Api response is null or invaild.	The response is empty.	Ensure that the backend server is healthy.
400	ELB.0230	Tenant_id is empty.	The project ID is left blank.	Correct the project ID.
400	ELB.1000	The loadbalancer URL is too long.	The URL length exceeds the limit.	Correct the URL.
400	ELB.1001	Request parameters invalid.	Invalid parameters.	Enter valid parameters.
400	ELB.1003	Lb not exist.	The load balancer does not exist.	Check the load balancer ID.

Status Code	Error Codes	Error Message	Description	Solution
400	ELB.1004	Query condition is not valid.	Invalid query condition.	Change the query condition.
400	ELB.1005	Update request paramters error.	Failed to modify the load balancer.	Check the parameters.
400	ELB.1007	Query internal ELB error.	Failed to query details of the private network load balancer.	Contact customer service.
400	ELB.1008	There is at least one member under the lb.	Failed to delete the load balancer.	Change the parameter settings.
400	ELB.1010	Query elb quota error.	Failed to query the quota.	Contact customer service.
400	ELB.1011	Private_key or certificate content is not valid.	Invalid private or public key of the server certificate.	Enter a valid private or public key.
400	ELB.1012	Create tenant resource relation error.	Failed to create the relationship between resources and the user.	Contact customer service.
400	ELB.1013	Update resource tenant allocation failed, cloud eye warning rule exceeds.	Failed to modify the quota of a resource because the quota set in the Cloud Eye alarm rule is too large.	Contact customer service.
400	ELB.1014	Query resouce tenant relation failed.	Failed to query the relationship between resources and the user.	Contact customer service.

Status Code	Error Codes	Error Message	Description	Solution
400	ELB.1015	Lb can not be updated.	Failed to modify the load balancer.	Check the parameters.
400	ELB.1018	There is at least one member under the lb.	Failed to delete the load balancer because it has backend servers associated.	Remove the backend servers from the associated backend server group and delete the backend server group first.
400	ELB.1020	Lb ID is not correct.	Incorrect load balancer ID.	Change the parameter settings.
400	ELB.1021	Request parameters error, name invalid.	Invalid load balancer name.	Change the name.
400	ELB.1025	Udpate request parameters error, name is too long.	The load balancer name exceeds the length limit.	Change the name.
400	ELB.1031	Request parameters error, lb len description too long.	The load balancer description exceeds the length limit.	Change the description.
400	ELB.1035	Update request parameters error, name is not valid.	Invalid load balancer name.	Change the name.
400	ELB.1041	Request parameters error, lb type is not valid.	Invalid load balancer type.	Change the parameter settings.
400	ELB.1045	Update request parameters error, description too long.	The load balancer description exceeds the length limit.	Change the description.

Status Code	Error Codes	Error Message	Description	Solution
400	ELB.1051	Request parameters error, lb bandwidth is not valid.	Invalid bandwidth configured for the load balancer.	Modify the bandwidth.
400	ELB.1061	Request parameters error, lb vip_address and vip_subnet_id are nil.	The EIP or subnet ID is left blank.	Enter a valid EIP or subnet ID.
400	ELB.1071	Request parameters error, lb vip_address is not valid.	Invalid EIP.	Enter a valid EIP.
400	ELB.1081	Request parameters error, lb vpc_id is empty.	The VPC ID is left blank.	Enter a valid VPC ID.
400	ELB.1101	Vip address is exist.	The EIP already exists.	Enter another EIP.
400	ELB.1110	version not found.	The API version does not exist.	Contact customer service.
400	ELB.1201	Get Token failed	Failed to obtain the token.	Contact customer service.
400	ELB.1202	enterprise_project_id can not be empty	An error occurred during the verification of ep_id.	Check the enterprise project ID.
400	ELB.1204	Bind fail.	Failed to associate the load balancer with the enterprise project.	Contact customer service.

Status Code	Error Codes	Error Message	Description	Solution
400	ELB.2002	Delete member input param error.	Failed to remove the backend server because the parameters are invalid.	Change the parameter settings.
400	ELB.2003	Query member failed.	Failed to query the backend server.	Contact customer service.
400	ELB.2005	Update member failed.	Failed to update the backend server.	Contact customer service.
400	ELB.2010	Member listener ID length is not correct.	The listener ID exceeds the length limit.	Change the listener ID.
400	ELB.2011	Add member listener is not exist.	The listener does not exist.	Ensure that the listener exists.
400	ELB.2012	This member is not exist.	The backend server does not exist.	Ensure that the backend server exists.
400	ELB.2020	Member listener ID content is not correct.	Invalid listener ID.	Change the listener ID.
400	ELB.2021	Request parameters error, member address is null.	Invalid backend server IP address.	Check the backend server IP address.
400	ELB.3001	Create floating IP failed.	Failed to assign the EIP.	Contact customer service.
400	ELB.3002	Delete floating IP failed.	Failed to release the EIP.	Contact customer service.

Status Code	Error Codes	Error Message	Description	Solution
400	ELB.3003	Query floating IP failed.	Failed to query the EIP.	Contact customer service.
400	ELB.3004	Query floating IP list failed.	Failed to query EIPs.	Contact customer service.
400	ELB.4001	Create elastic IP failed.	Failed to assign the EIP.	Contact customer service.
400	ELB.4002	Delete elastic IP failed.	Failed to release the EIP.	Contact customer service.
400	ELB.4003	Query elastic IP failed.	Failed to query the EIP.	Contact customer service.
400	ELB.4004	Query elastic IP list failed.	Failed to query EIPs.	Contact customer service.
400	ELB.4005	Update elastic IP failed.	Failed to update the EIP.	Contact customer service.
400	ELB.5002	Failed to delete the certificate.	Failed to delete the certificate.	Contact customer service.
400	ELB.5003	Query bandwidth failed.	Failed to query the bandwidth.	Contact customer service.
400	ELB.5004	Invalid search criteria.	Invalid query condition.	Change the query condition.
400	ELB.5005	Update bandwidth failed.	Failed to modify the bandwidth.	Contact customer service.
400	ELB.5013	Private_key or certificate content is not valid.	Invalid public or private key of the server certificate.	Enter a valid public or private key.
400	ELB.5020	The certificate ID must be 32 characters.	The certificate ID is not a 32-character string.	Enter a valid certificate ID.
400	ELB.5033	Failed to update certificate.	Failed to modify the certificate.	Contact customer service.

Status Code	Error Codes	Error Message	Description	Solution
400	ELB.5040	The certificate does not exist.	The certificate does not exist.	Ensure that the certificate exists.
400	ELB.5051	CA certificate content is not valid.	Invalid CA certificate body.	Enter a valid certificate body.
400	ELB.5053	CA certificate content is not valid.	Invalid CA certificate body.	Enter a valid certificate body.
400	ELB.5131	Failed to query the certificate quota.	Failed to query the certificate quota.	Contact customer service.
400	ELB.5141	Failed to query the user certificate quota.	Failed to query the used certificate quota.	Contact customer service.
400	ELB.5151	The certificate quantity exceeds the quota.	The certificate quota has been used up.	Delete the certificates that are no longer used or request a higher quota.
400	ELB.6010	Listener ID content is not correct.	Invalid listener ID.	Change the listener ID.
400	ELB.6011	Request parameters error, listener name too long.	The listener name exceeds the length limit.	Change the name.
400	ELB.6015	This listener prerty cannot be updated	The listener property cannot be modified.	Select a property that can be modified.
400	ELB.6021	Request parameters error, listener name is not valid.	Invalid listener name.	Change the name.

Status Code	Error Codes	Error Message	Description	Solution
400	ELB.6025	Udpate request parameters error, listener len name too long.	The listener name exceeds the length limit.	Change the name.
400	ELB.6030	Listener is not associated with loadbalancer id.	The listener does not belong to any load balancer.	Check the listener ID.
400	ELB.6031	Request parameters error, listener len description too long.	The listener description exceeds the length limit.	Change the description.
400	ELB.6035	Udpate request parameters error, listener name is not valid.	Invalid listener name.	Change the name.
400	ELB.6040	The loadbalaner that the listener belongs to is not exist.	The load balancer to which the listener is added does not exist.	Check the load balancer ID.
400	ELB.6041	Request parameters error, listener port is not in 1 ~ 65535.	Invalid port number.	Change the port number.
400	ELB.6045	Update request parameters error, listener len description too long.	The listener description exceeds the length limit.	Change the description.

Status Code	Error Codes	Error Message	Description	Solution
400	ELB.6051	Request parameters error, listener lb algorithm is not valid.	Invalid load balancing algorithm.	Change the load balancing algorithm.
400	ELB.6061	Request parameters error, listener protocol is not valid.	Invalid listener protocol.	Change the protocol.
400	ELB.6071	Request parameters error, listener backend protocol is not valid.	Invalid backend server protocol.	Change the protocol.
400	ELB.6200	Load Balaner *** already has a listener with protocol_port of ***.	The port number is in use.	Change the port number.
400	ELB.7000	Listener_id must not be null.	The listener ID is left blank.	Change the listener ID.
400	ELB.7001	Healthcheck_interval is illegal.	Invalid query condition.	Change the query condition.
400	ELB.7002	Healthcheck delete condition is not valid.	Invalid query condition.	Change the query condition.
400	ELB.7004	Healthcheck query condition is not valid.	Invalid query condition.	Change the query condition.
400	ELB.7010	Healthcheck listener is not exist.	The listener with which the health check is associated does not exist.	Change the listener ID.

Status Code	Error Codes	Error Message	Description	Solution
400	ELB.7014	Healthcheck configuration not exist.	The health check does not exist.	Check the health check ID.
400	ELB.7020	This healthcheck is not exist.	The health check does not exist.	Change the health check ID.
400	ELB.8001	Create a SG error.	Failed to create the security group.	Contact customer service.
400	ELB.8101	Create VPC error.	Failed to create the VPC.	Contact customer service.
400	ELB.8102	Delete VPC error.	Failed to delete the VPC.	Contact customer service.
400	ELB.8103	Query VPC error.	Failed to query the VPC.	Contact customer service.
400	ELB.8201	Create subnet error.	Failed to create the subnet.	Contact customer service.
400	ELB.8202	Delete subnet error.	Failed to delete the subnet.	Contact customer service.
400	ELB.8203	Query subnet error.	Failed to query the subnet.	Contact customer service.
400	ELB.8902	Invalid input for '%s' is not in %s.	Invalid input parameters.	Check input parameters.
400	ELB.8909	Certificate with multi domain not supported by guaranteed listener.	Multiple domain certificate is not supported by dedicated loadbalancer.	Check input parameters.

Status Code	Error Codes	Error Message	Description	Solution
400	ELB.8934	The number of available IP addresses in the subnet on the downstream plane is insufficient.	The elb_virsubnet_ids %s is expected to use %s ipv4 addresses but only %s ipv4 addresses are available, Please reselect.	Check your request based on the error message.
400	ELB.8938	The ip member just support when pool's protocol is %s.	Invalid input parameters.	Change the value of pool_id in url to other suppprted pool or pass parameter 'subnet_cidr_id' when create member.
400	ELB.8939	The loadbalancer's ip_target_enable must be true when add ip member.	Invalid input parameters.	Disable ip target of the loadbalancer or pass parameter 'subnet_cidr_id' when create member.
400	ELB.8950	Cannot allocate resource for the loadbalancer.	Cannot allocate resource for the loadbalancer.	Contact customer service.
400	ELB.8959	The %s flavor field does not support update from %s to %s.	Invalid input parameters when updating flavor.	Check input parameters.
400	ELB.9001	Interval ELB create VM error.	Failed to create the VM.	Contact customer service.
400	ELB.9002	Internal ELB delete VM error.	Failed to delete the VM.	Contact customer service.
400	ELB.9003	Internal ELB query VM error.	Failed to query details of the VM.	Contact customer service.

Status Code	Error Codes	Error Message	Description	Solution
400	ELB.9006	Internal ELB update port fail.	Failed to update the port bound to the VM.	Contact customer service.
400	ELB.9007	Intenal ELB bind port fail.	Failed to bind the port to the VM.	Contact customer service.
400	ELB.9023	Internal ELB get image error.	Failed to query the image.	Contact customer service.
400	ELB.9033	Internal ELB get flavour error.	Failed to query the VM specifications.	Contact customer service.
400	ELB.9043	Internal ELB get interface error.	Failed to query the port bound to the VM.	Contact customer service.
400	ELB.9061	Internal ELB query topic fail.	Failed to query the SMN topic.	Contact customer service.
400	ELB.9062	Internal ELB create topic fail.	Failed to create the SMN topic.	Contact customer service.
400	ELB.9063	Internal ELB query subscription fail.	Failed to query the SMN subscription.	Contact customer service.
400	ELB.9064	Internal ELB create subscription fail.	Failed to create the SMN subscription.	Contact customer service.
400	ELB.9800	Resource could not be found.	The specified load balancer does not exist when ep_id is queried.	Ensure that the load balancer belongs to the enterprise project.

Status Code	Error Codes	Error Message	Description	Solution
400	ELB.9801	Not be list action, enterprise_project_id must not be null.	In fine-grained authorization, the enterprise ID is not passed in the request for querying load balancers.	Ensure that the parameters in the request for querying load balancers are correct.
400	ELB.9805	RequestBody listener[protocol] is null, this is a required parameter.	ep_id in the URI is not a valid UUID.	Check the enterprise project ID.
400	ELB.9807	Quota exceeded for resources: %s	No enought quota for resource.	Contact customer to expand quota.
400	ELB.9899	Invalid parameter. For details about the error, see the returned information.	Invalid parameter. For details about the error, see the returned information.	Please check parameters.
401	ELB.1103	Token invalid	Invalid token.	Contact customer service.
401	ELB.1104	Token invalid	Invalid token.	Contact customer service.
401	ELB.1105	Token invalid	Invalid token.	Contact customer service.
401	ELB.1109	Authentication failed.	Real-name authentication failed.	Contact customer service.
403	ELB.1091	Lb number larger than quota.	The number of load balancers exceeds the quota.	Request a higher quota or delete load balancers that are no longer needed.
403	ELB.1102	Token is error, Authentication required.	The token is empty.	Enter a token that has not expired.

Status Code	Error Codes	Error Message	Description	Solution
403	ELB.2001	Create member failed, the total amount of members exceeds the system setting.	Failed to add the backend server because the number of backend servers reaches the limit.	Check the maximum number of backend servers.
403	ELB.6091	Request lb has more than user listener quota.	The number of listeners reaches the limit.	Request a higher quota or delete listeners that are no longer needed.
403	ELB.8962	tenant %s does not support %s.	The feature is not supported.	Contact customer service.
403	ELB.9802	Policy doesn't allow elb:logtanks:create to be performed.	Authentication failed.	Ensure that you have the permission to perform this operation.
403	ELB.9803	Policy doesn't allow elb:loadbalancers:list to be performed.	Authentication failed.	Ensure that you have the permission to perform this operation.
403	ELB.9804	Policy doesn't allow elb:loadbalancers:list to be performed.	Authentication failed.	Ensure that you have the permission to perform this operation.
404	ELB.1002	Find lb failed.	The load balancer does not exist.	Change the load balancer ID.
404	ELB.8904	%s %s could not be found.	Resource could not be found.	Please check the parameters.
409	ELB.8905	Quota exceeded for resources: %s	No enough quota for resource.	Contact customer to expand quota.

Status Code	Error Codes	Error Message	Description	Solution
409	ELB.8907	Data conflict. For details about the error, see the returned information.	Data conflict. For details about the error, see the returned information.	Check your request based on the error message.
500	ELB.8906	Internal error. For details about the error, see the returned information.	Internal error. For details about the error, see the returned information.	Contact customer service.

A.2 Status Codes

Table A-1 Normal status codes

Status Code	Message	Description
200	OK	Normal response to GET and PUT requests.
201	Created	Normal response to POST requests.
204	No Content	Normal response to DELETE requests.

Table A-2 Error codes

Status Code	Message	Description
400	Bad Request	Invalid request URI.
		Too long request header.
		Invalid request body.
		Unreleased fields in the request body.
401	Unauthorized	Authentication information unavailable in the request header.
		Expired authentication information in the request header.
403	Forbidden	No permissions to access APIs.

Status Code	Message	Description
404	Not Found	No available request URI.
		No available requested resources.
405	Method Not Allowed	Method specified in the request not allowed.
406	Not Acceptable	Responses from the server failed to be received by the client.
407	Proxy Authentication Required	Proxy authentication required before the request can be processed.
408	Request Timeout	Request timed out.
409	Conflict	Failed to complete the request due to conflicts.
		The resource being accessed by another request.
500	Internal IaaS OpenStack network error.	Service internal error.
		Server exception.
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 receives an invalid response from the upstream server.
503	Service Unavailable	Failed to complete the request because the system is temporarily abnormal.
504	Gateway Timeout	Gateway timed out.

A.3 General Information About Shared Load Balancers

The following information applies only to shared load balancers.

A.3.1 Querying Data in Pages

APIs v2.0 allow users to query data in pages by adding the limit and marker parameters to the URL of the list request. The query results are displayed in the ascending order of IDs.

- **next ref** in the response indicates the URL of the next page.
- **previous ref** in the response indicates the URL of the previous page.

Request

Table A-3 Parameter description

Parameter	Type	Mandatory	Description
limit	int	No	Specifies the number of records on each page.
marker	String	No	Specifies the resource ID of pagination query. If the parameter is left blank, only resources on the first page are queried.
page_reverse	Bool	No	Specifies the paging sequence. The value can be **true** or **false**.

Response

None

Example

- Example request
  ```
  GET /v2.0/networks?limit=2&marker=3d42a0d4-a980-4613-ae76-a2cddecff054&page_reverse=False
  ```
- Example response
  ```
  {
     "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"
        }
     ]
  }
  ```


A.3.2 Sequencing Query Results

API v2.0 enables the system to sort queried results based on customized keys by adding the **sort_key** and **sort_dir** parameters to the URL of the list request.

sort_key specifies the parameter used for sequencing results, and **sort_dir** specifies whether results are displayed in ascending or descending order.

These APIs allow sorting query results by multiple criteria. The number of **sort_key** parameters must be equal to that of **sort_dir** parameters. Otherwise, 400 status code is returned.

Example Request

```
GET /v2.0/networks?sort_key=name&sort_dir=asc&sort_key=status&sort_dir=desc
```

Example Response

```
{
   "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"
      },
      {
         "status": "ACTIVE",
         "subnets": [
            "e25189a8-54df-4948-9396-d8291ffc92a0"
         ],
         "name": "testnet01",
         "admin_state_up": true,
         "tenant_id": "6fbe9263116a4b68818cf1edce16bc4f",
         "id": "3d42a0d4-a980-4613-ae76-a2cddecff054"
      }
   ]
}
```

A.3.3 Basic Workflow

The basic workflow of sharedload balancers contains the following: creating a load balancer, adding a listener to a specific load balancer, adding a backend server group to a specific listener, configuring a health check for a specific backend server group, and adding a backend server to a specific backend server group. Deletion operations include removing a backend server, deleting a health check, deleting a backend server group, deleting a listener, and deleting a load balancer.

Provision Resources

- Creating a load balancer
- Adding a listener to a specific load balancer
- Adding a backend server group to a specific listener
- Configuring a health check for a specific backend server group
- Adding a backend server to a specific backend server group

Reclaim Resources

- Removing a backend server
- Deleting a health check
- Deleting a backend server group
- Deleting a listener
- Deleting a load balancer

A.4 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