

Elastic Load Balance

API Reference

Issue	01
Date	2025-09-19



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

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

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Contents

1 Before You Start..... 1

2 API Overview..... 4

3 Selecting an API Version..... 7

4 Calling APIs..... 8

4.1 Making an API Request..... 8

4.2 Authentication..... 12

4.3 Response..... 13

5 APIs (V3)..... 16

5.1 API Version..... 16

5.1.1 Querying API Versions..... 16

5.2 Quota..... 20

5.2.1 Querying Quotas..... 20

5.2.2 Querying Quota Usage..... 29

5.3 AZ..... 35

5.3.1 Querying AZs..... 36

5.4 Load Balancer Flavor..... 42

5.4.1 Querying Flavors..... 42

5.4.2 Viewing the Details of a Flavor..... 55

5.5 Reserved IP Address..... 63

5.5.1 Calculating the Number of Reserved IP Addresses..... 63

5.6 Load Balancer..... 76

5.6.1 Creating a Load Balancer..... 76

5.6.2 Batch Creating Load Balancers..... 119

5.6.3 Upgrading a Load Balancer..... 147

5.6.4 Querying Load Balancers..... 156

5.6.5 Copying a Load Balancer..... 189

5.6.6 Viewing the Details of a Load Balancer..... 200

5.6.7 Updating a Load Balancer..... 216

5.6.8 Deleting a Load Balancer..... 246

5.6.9 Deleting a Load Balancer and Its Associated Resources..... 250

5.6.10 Deleting a Load Balancer and Its Associated Resources (Including EIPs)..... 254

5.6.11 Querying the Status Tree of a Load Balancer..... 260

5.6.12 Querying the Ports on the Downstream Subnet Used by a Load Balancer.....	271
5.6.13 Deploying a Load Balancer in Additional AZs.....	277
5.6.14 Removing a Load Balancer from AZs.....	294
5.7 Certificate.....	312
5.7.1 Creating a Certificate.....	312
5.7.2 Querying Certificates.....	329
5.7.3 Querying the Details of a Certificate.....	345
5.7.4 Updating a Certificate.....	353
5.7.5 Deleting a Certificate.....	365
5.7.6 Enabling or Disabling the Private Key Feature.....	369
5.7.7 Querying Whether the Private Key Feature Is Enabled.....	374
5.8 Security Policy.....	379
5.8.1 Creating a Custom Security Policy.....	379
5.8.2 Querying Custom Security Policies.....	388
5.8.3 Querying the Details of a Custom Security Policy.....	397
5.8.4 Updating a Custom Security Policy.....	402
5.8.5 Deleting a Custom Security Policy.....	411
5.8.6 Querying System Security Policies.....	415
5.9 IP Address Group.....	421
5.9.1 Creating an IP Address Group.....	421
5.9.2 Querying IP Address Groups.....	430
5.9.3 Querying the Details of an IP Address Group.....	440
5.9.4 Updating an IP Address Group.....	446
5.9.5 Deleting an IP Address Group.....	454
5.9.6 Updating IP Addresses in an IP Address Group.....	458
5.9.7 Deleting IP Addresses from an IP Address Group.....	467
5.9.8 Querying the Listeners Associated with an IP Address Group.....	474
5.10 Listener.....	479
5.10.1 Adding a Listener.....	479
5.10.2 Querying Listeners.....	518
5.10.3 Viewing the Details of a Listener.....	544
5.10.4 Updating a Listener.....	560
5.10.5 Deleting a Listener.....	593
5.10.6 Deleting a Listener and Its Associated Resources.....	597
5.11 Backend Server Group.....	601
5.11.1 Creating a Backend Server Group.....	601
5.11.2 Querying Backend Server Groups.....	637
5.11.3 Querying the Details of a Backend Server Group.....	662
5.11.4 Updating a Backend Server Group.....	678
5.11.5 Deleting a Backend Server Group.....	708
5.11.6 Deleting a Backend Server Group and Associated Resources.....	712
5.12 Backend Server.....	716

5.12.1 Adding a Backend Server.....	716
5.12.2 Querying Backend Servers in a Backend Server Group.....	734
5.12.3 Viewing the Details of a Backend Server.....	753
5.12.4 Updating a Backend Server.....	764
5.12.5 Removing a Backend Server.....	779
5.12.6 Querying Backend Servers in a Project.....	783
5.12.7 Batch Adding Backend Servers.....	804
5.12.8 Batch Removing Backend Servers.....	819
5.12.9 Batch Updating Backend Servers.....	829
5.12.10 Creating a Backend Server Check Task.....	844
5.12.11 Querying the Results of a Backend Server Check Task.....	849
5.13 Health Check.....	858
5.13.1 Configuring a Health Check.....	858
5.13.2 Querying Health Checks.....	871
5.13.3 Viewing the Details of a Health Check.....	884
5.13.4 Updating a Health Check.....	891
5.13.5 Deleting a Health Check.....	904
5.14 Forwarding Policy.....	908
5.14.1 Adding a Forwarding Policy.....	908
5.14.2 Querying Forwarding Policies.....	955
5.14.3 Querying the Details of a Forwarding Policy.....	977
5.14.4 Modifying a Forwarding Policy.....	993
5.14.5 Deleting a Forwarding Policy.....	1038
5.14.6 Batch Modifying Forwarding Policy Priorities.....	1042
5.15 Forwarding Rule.....	1049
5.15.1 Adding a Forwarding Rule.....	1049
5.15.2 Querying Forwarding Rules.....	1067
5.15.3 Viewing the Details of a Forwarding Rule.....	1082
5.15.4 Updating a Forwarding Rule.....	1092
5.15.5 Deleting a Forwarding Rule.....	1110
5.16 Active/Standby Backend Server Group.....	1114
5.16.1 Creating an Active/Standby Backend Server Group.....	1114
5.16.2 Querying Active/Standby Backend Server Groups.....	1147
5.16.3 Viewing the Details of an Active/Standby Backend Server Group.....	1172
5.16.4 Deleting an Active/Standby Backend Server Group.....	1190
5.17 Log.....	1194
5.17.1 Creating a Log.....	1194
5.17.2 Querying Logs.....	1200
5.17.3 Viewing the Details of a Log.....	1208
5.17.4 Updating a Log.....	1213
5.17.5 Deleting a Log.....	1218
5.18 Asynchronous Task.....	1222

5.18.1 Querying the Asynchronous Tasks.....	1222
5.18.2 Querying the Status of an Asynchronous Task.....	1231
5.19 Feature Configuration.....	1237
5.19.1 Querying the Feature Configurations of ELB.....	1237
5.19.2 Querying the Feature Configurations of a Load Balancer.....	1243
5.20 Recycle Bin.....	1248
5.20.1 Enabling or Disabling Recycle Bin.....	1248
5.20.2 Querying the Recycle Bin Policy.....	1253
5.20.3 Updating the Recycle Bin Policy.....	1258
5.20.4 Querying Load Balancers in the Recycle Bin.....	1264
5.20.5 Restoring a Load Balancer from the Recycle Bin.....	1289
5.20.6 Permanently Deleting a Load Balancer from the Recycle Bin.....	1293
6 APIs (V2).....	1298
6.1 Load Balancer.....	1298
6.1.1 Creating a Load Balancer.....	1298
6.1.2 Querying Load Balancers.....	1306
6.1.3 Querying Details of a Load Balancer.....	1314
6.1.4 Querying the Status Tree of a Load Balancer.....	1319
6.1.5 Updating a Load Balancer.....	1327
6.1.6 Deleting a Load Balancer.....	1334
6.2 Listener.....	1335
6.2.1 Adding a Listener.....	1335
6.2.2 Querying Details of a Listener.....	1349
6.2.3 Querying Listeners.....	1355
6.2.4 Updating a Listener.....	1366
6.2.5 Deleting a Listener.....	1378
6.3 Backend Server Group.....	1379
6.3.1 Adding a Backend Server Group.....	1379
6.3.2 Querying Backend Server Groups.....	1390
6.3.3 Querying Details of a Backend Server Group.....	1399
6.3.4 Updating a Backend Server Group.....	1405
6.3.5 Deleting a Backend Server Group.....	1414
6.4 Backend Server.....	1415
6.4.1 Adding a Backend Server.....	1415
6.4.2 Querying Backend Servers.....	1419
6.4.3 Querying Details of a Backend Server.....	1425
6.4.4 Updating a Backend Server.....	1428
6.4.5 Removing a Backend Server.....	1432
6.5 Health Check.....	1433
6.5.1 Configuring a Health Check.....	1433
6.5.2 Querying Health Checks.....	1440
6.5.3 Querying Health Check Details.....	1447

6.5.4 Updating a Health Check.....	1450
6.5.5 Deleting a Health Check.....	1456
6.6 Forwarding Policy.....	1457
6.6.1 Adding a Forwarding Policy.....	1457
6.6.2 Querying Forwarding Policies.....	1464
6.6.3 Querying Details of a Forwarding Policy.....	1470
6.6.4 Updating a Forwarding Policy.....	1473
6.6.5 Deleting a Forwarding Policy.....	1477
6.7 Forwarding Rule.....	1477
6.7.1 Adding a Forwarding Rule.....	1478
6.7.2 Querying Forwarding Rules.....	1483
6.7.3 Querying Details of a Forwarding Rule.....	1488
6.7.4 Updating a Forwarding Rule.....	1491
6.7.5 Deleting a Forwarding Rule.....	1495
6.8 Whitelist.....	1496
6.8.1 Adding a Whitelist.....	1496
6.8.2 Querying Details of a Whitelist.....	1499
6.8.3 Querying Whitelists.....	1500
6.8.4 Updating a Whitelist.....	1503
6.8.5 Deleting a Whitelist.....	1506
6.9 Certificate.....	1507
6.9.1 Creating a Certificate.....	1507
6.9.2 Querying Certificates.....	1513
6.9.3 Querying Details of a Certificate.....	1522
6.9.4 Updating a Certificate.....	1526
6.9.5 Deleting a Certificate.....	1532
7 APIs (OpenStack).....	1534
7.1 Tag.....	1534
7.1.1 Adding a Tag to a Load Balancer.....	1534
7.1.2 Batch Adding Load Balancer Tags.....	1536
7.1.3 Batch Deleting Load Balancer Tags.....	1538
7.1.4 Querying All Tags of a Load Balancer.....	1541
7.1.5 Querying the Tags of All Load Balancers.....	1542
7.1.6 Querying Load Balancers by Tag.....	1544
7.1.7 Deleting a Tag from a Load Balancer.....	1549
7.1.8 Adding a Tag to a Listener.....	1550
7.1.9 Batch Adding Tags to a Listener.....	1552
7.1.10 Batch Deleting Tags from a Listener.....	1554
7.1.11 Querying All Tags of a Listener.....	1556
7.1.12 Querying the Tags of All Listeners.....	1558
7.1.13 Querying Listeners by Tag.....	1560
7.1.14 Deleting a Tag from a Listener.....	1565

7.1.15 Status Codes.....	1566
8 Examples.....	1569
8.1 Creating a Dedicated Load Balancer and Binding a New EIP to It.....	1569
8.2 Adding a Listener to a Dedicated Load Balancer.....	1571
8.3 Deleting a Dedicated Load Balancer.....	1572
8.4 Creating a Public Network (Shared) Load Balancer.....	1575
8.5 Querying the ID of an ECS Used as a Backend Server.....	1580
9 Permissions and Supported Actions.....	1582
9.1 Introduction.....	1582
9.2 Supported Actions (V2).....	1583
9.2.1 Load Balancer.....	1583
9.2.2 Listener.....	1584
9.2.3 Backend Server Group.....	1585
9.2.4 Backend Server.....	1585
9.2.5 Health Check.....	1586
9.2.6 Forwarding Policy.....	1587
9.2.7 Forwarding Rule.....	1588
9.2.8 Whitelist.....	1588
9.2.9 SSL Certificate.....	1589
9.2.10 Quota.....	1590
9.2.11 Tag.....	1590
9.2.12 Precautions for API Permissions.....	1591
9.3 Supported Actions (V3).....	1592
9.3.1 Load Balancer.....	1592
9.3.2 Listener.....	1593
9.3.3 Backend Server Group.....	1593
9.3.4 Backend Server.....	1594
9.3.5 Health Check.....	1595
9.3.6 Forwarding Policy.....	1596
9.3.7 Forwarding Rule.....	1596
9.3.8 IP Address Group.....	1597
9.3.9 Certificate.....	1598
9.3.10 Security Policy.....	1599
9.3.11 Quota.....	1600
9.3.12 API Version.....	1601
9.3.13 Availability Zone.....	1601
9.3.14 Load Balancer Flavor.....	1601
9.3.15 Precautions for API Permissions.....	1601
10 Historical APIs.....	1603
10.1 Shared Load Balancer APIs (OpenStack) (Discarded).....	1603
10.1.1 Load Balancer.....	1603

10.1.1.1 Creating a Load Balancer.....	1603
10.1.1.2 Querying Load Balancers.....	1614
10.1.1.3 Querying Details of a Load Balancer.....	1620
10.1.1.4 Querying the Status Tree of a Load Balancer.....	1623
10.1.1.5 Updating a Load Balancer.....	1631
10.1.1.6 Deleting a Load Balancer.....	1635
10.1.2 Listener.....	1636
10.1.2.1 Adding a Listener.....	1636
10.1.2.2 Querying Listeners.....	1645
10.1.2.3 Querying Details of a Listener.....	1656
10.1.2.4 Updating a Listener.....	1659
10.1.2.5 Deleting a Listener.....	1666
10.1.3 Backend Server Group.....	1667
10.1.3.1 Adding a Backend Server Group.....	1667
10.1.3.2 Querying Backend Server Groups.....	1678
10.1.3.3 Querying Details of a Backend Server Group.....	1686
10.1.3.4 Updating a Backend Server Group.....	1691
10.1.3.5 Deleting a Backend Server Group.....	1699
10.1.4 Backend Server.....	1700
10.1.4.1 Adding a Backend Server.....	1700
10.1.4.2 Querying Backend Servers.....	1705
10.1.4.3 Querying Details of a Backend Server.....	1710
10.1.4.4 Updating a Backend Server.....	1713
10.1.4.5 Removing a Backend Server.....	1717
10.1.5 Health Check.....	1718
10.1.5.1 Configuring a Health Check.....	1718
10.1.5.2 Querying Health Checks.....	1725
10.1.5.3 Querying Details of a Health Check.....	1733
10.1.5.4 Updating a Health Check.....	1736
10.1.5.5 Deleting a Health Check.....	1742
10.1.6 Forwarding Policy.....	1743
10.1.6.1 Adding a Forwarding Policy.....	1743
10.1.6.2 Querying Forwarding Policies.....	1751
10.1.6.3 Querying Details of a Forwarding Policy.....	1758
10.1.6.4 Updating a Forwarding Policy.....	1760
10.1.6.5 Deleting a Forwarding Policy.....	1764
10.1.7 Forwarding Rule.....	1765
10.1.7.1 Adding a Forwarding Rule.....	1765
10.1.7.2 Querying Forwarding Rules.....	1771
10.1.7.3 Querying Details of a Forwarding Rule.....	1777
10.1.7.4 Updating a Forwarding Rule.....	1780
10.1.7.5 Deleting a Forwarding Rule.....	1784

10.1.8 Whitelist.....	1784
10.1.8.1 Adding a Whitelist.....	1784
10.1.8.2 Querying Whitelists.....	1787
10.1.8.3 Querying Details of a Whitelist.....	1790
10.1.8.4 Updating a Whitelist.....	1792
10.1.8.5 Deleting a Whitelist.....	1794
10.1.9 Certificate.....	1795
10.1.9.1 Creating a Certificate.....	1795
10.1.9.2 Querying Certificates.....	1800
10.1.9.3 Querying Details of a Certificate.....	1809
10.1.9.4 Updating a Certificate.....	1813
10.1.9.5 Deleting a Certificate.....	1818
10.2 Asynchronous Job Query (Discarded).....	1819
10.3 Querying Versions (Discarded).....	1821
10.4 Getting Started.....	1822
10.4.1 Creating a Load Balancer.....	1822
10.4.2 Obtaining a Token.....	1823
10.4.3 Creating a Load Balancer.....	1823
10.4.4 Creating a Public Network Load Balancer.....	1825
10.4.5 Adding a Listener.....	1829
10.4.6 Creating a Backend Server Group.....	1830
10.4.7 Adding Backend Servers.....	1832
10.4.8 Configuring a Health Check.....	1834
10.4.9 Adding a Forwarding Policy.....	1836
10.4.10 Adding a Forwarding Rule.....	1838
10.4.11 Adding a Whitelist.....	1839
10.4.12 Creating an SSL Certificate.....	1840
A Appendix.....	1844
A.1 Error Codes.....	1844
A.2 Status Codes.....	1858
A.3 General Information About Shared Load Balancers.....	1859
A.3.1 Querying Data in Pages.....	1859
A.3.2 Sequencing Query Results.....	1861
A.3.3 Basic Workflow.....	1861
A.4 Obtaining a Project ID.....	1862

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](#).

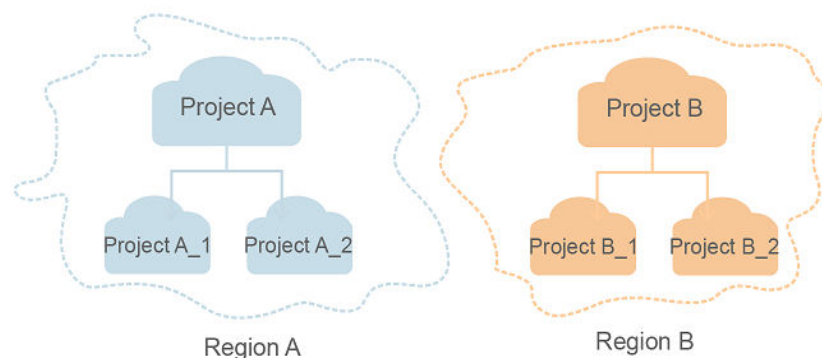
- AZ

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, and deletes a load balancer, queries 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, queries the details of a certificate, and lists certificates.
	Security policy	Adds, modifies, and deletes a security policy, queries the details of a security policy, and lists security policies.
	IP address group	Configures, modifies, and deletes an IP address group, queries the details of an IP address group, and lists IP address groups.
	Listener	Adds, modifies, and deletes a listener, queries the details of a listener, and lists listeners.
	Backend server group	Adds, modifies, and deletes a backend server group, queries the details of a backend server group, and lists backend server groups.
	Backend server	Adds, modifies, and deletes a backend server, queries the details of a backend server, and lists backend servers.
	Health check	Configures, modifies, and disables a health check, queries the details of a health check, and lists health checks.

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

Type	Resource	Description
	Backend server group	Adds, updates, and deletes a backend server group, queries the details of a backend server group, and lists backend server groups.
	Backend server	Adds, updates, and removes a backend server, queries the details of a backend server, and lists backend servers.
	Health check	Configures, updates, and disables a health check, queries the details of a health check, and lists health checks.
	Forwarding policy	Adds, updates, and deletes a forwarding policy, queries the details of a forwarding policy, and lists forwarding policies.
	Forwarding rule	Adds, updates, and deletes a forwarding rule, queries the details of a forwarding rule, and lists forwarding rules.
	Whitelist	Creates, updates, and deletes a whitelist, queries the details of a whitelist, and lists whitelists.
	SSL certificate	Creates, modifies, deletes a certificate, queries the details of 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 a tag to and deletes a tag from a listener, batch adds and deletes listener tags, 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.

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

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

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

Figure 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.
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 <i>Hostname:Port number</i> . If the port number is not specified, the default port is used. The default port number for https is 443 .	No This field is mandatory for AK/SK authentication.	code.test.com or code.test.com:443
Content-Type	Specifies the type (or format) of the message body. The default value application/json is recommended. Other values of this field will be provided for specific APIs if any.	Yes	application/json
Content-Length	Specifies the length of the request body. The unit is byte.	No	3495
X-Project-Id	Specifies the project ID. Obtain the project ID by following the instructions in Obtaining a Project ID .	No This field is mandatory for requests that use AK/SK authentication in the Dedicated Cloud (DeC) scenario or multi-project scenario.	e9993fc787d94b6c886cbaa340f9c0f4

Parameter	Description	Mandatory	Example Value
X-Auth-Token	Specifies the user token. It is a response to the API for obtaining a user token (This is the only API that does not require authentication). After the request is processed, the value of X-Subject-Token in the response header is the token value.	No This field is mandatory for token authentication.	The following is part of an example token: MIIPAgYJKoZlhvc NAQcCo...ggg1B BIINPXsidG9rZ

 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.

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

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

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

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

NOTE

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

Token Authentication

NOTE

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

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

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 that the IAM user belongs to
          }
        }
      }
    },
    "scope": {
      "project": {
        "name": "xxxxxxx" // Project name
      }
    }
  }
}
```

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

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_ null_af2953f2bcc67a42325a69a19e6c32a2",  
"Date": "Tue, 21 May 2024 09:03:40 GMT",  
"Content-Type": "application/json; charset=utf8"
```

(Optional) Response Body

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

The following shows part of the response body for the API used to [create an IAM user](#).

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

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

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

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

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. Generally, APIs of a later version (v3 is the latest version) support more features than those of an earlier version.

Note the following when using APIs of different versions:

- The API (POST /v3/{project_id}/elb/loadbalancers) cannot be used to create shared load balancers. To create a shared load balancer, you can call v2/v2.0 API, the API (/v3/{project_id}/elb/loadbalancers/batch-create) to batch create load balancers, or the API (/v3/{project_id}/elb/loadbalancers/{loadbalancer_id}/clone) to copy a load balancer.
- Other v3 APIs can be used to manage both dedicated and shared load balancers and their associated resources. For example, you can call the API (POST /v3/{project_id}/elb/listeners) to add a listener to a shared load balancer. However, some features of dedicated load balancers are not supported. For details, see each API description.

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	Definition: Specifies the available API version.

Table 5-2 ApiVersionInfo

Parameter	Type	Description
id	String	Definition: Specifies the API version. Range: The value can be v3 , v2 , or v2.0 in descending order.
status	String	Definition: Specifies the status of the API version. Range: • CURRENT: current version, which is the latest supported API version. • STABLE: stable version • DEPRECATED: discarded 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.ElClientBuilder().
            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. The API returns only the total quota, not the used quota. To query the used quota, you can call the API (GET /v3/{project_id}/elb/quotas/details) to query quota usage details.

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	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-4 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-5 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
quota	Quota object	Definition: 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	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Range: The value can contain a maximum of 32 characters, including digits and lowercase letters.

Parameter	Type	Description
loadbalancer	Integer	Definition: Specifies the load balancer quota. Range: • If the value is greater than or equal to 0, it indicates the current quota. • -1 indicates that the quota is not limited.
certificate	Integer	Definition: Specifies the certificate quota. Range: • If the value is greater than or equal to 0, it indicates the current quota. • -1 indicates that the quota is not limited.
listener	Integer	Definition: Specifies the listener quota. Range: • If the value is greater than or equal to 0, it indicates the current quota. • -1 indicates that the quota is not limited.
l7policy	Integer	Definition: Specifies the forwarding policy quota. Range: • If the value is greater than or equal to 0, it indicates the current quota. • -1 indicates that the quota is not limited.
condition_per_policy	Integer	Definition: Specifies the maximum number of forwarding conditions per forwarding policy. Range: • 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	Definition: Specifies the backend server group quota. Range: • If the value is greater than or equal to 0, it indicates the current quota. • -1 indicates that the quota is not limited.
healthmonitor	Integer	Definition: Specifies the health check quota. Range: • If the value is greater than or equal to 0, it indicates the current quota. • -1 indicates that the quota is not limited.
member	Integer	Definition: Specifies the backend server quota. Range: • If the value is greater than or equal to 0, it indicates the current quota. • -1 indicates that the quota is not limited.
members_per_pool	Integer	Definition: Specifies the maximum number of backend servers in a backend server group. Range: • If the value is greater than or equal to 0, it indicates the current quota. • -1 indicates that the quota is not limited.
listeners_per_pool	Integer	Definition: Specifies the maximum number of listeners that can be associated with a backend server group. Range: • 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
ipgroup	Integer	Definition: Specifies the IP address group quota. Range: - If the value is greater than or equal to 0, it indicates the current quota. -1 indicates that the quota is not limited.
ipgroup_bindings	Integer	Definition: Specifies the maximum number of listeners that can be associated with an IP address group. Range: - If the value is greater than or equal to 0, it indicates the current quota. -1 indicates that the quota is not limited.
ipgroup_max_length	Integer	Definition: Specifies the maximum number of IP entries that can be added to an IP address group. Range: - If the value is greater than or equal to 0, it indicates the current quota. -1 indicates that the quota is not limited.
security_policy	Integer	Definition: Specifies the custom security policy quota. Range: - If the value is greater than or equal to 0, it indicates the current quota. -1 indicates that the quota is not limited.
listeners_per_load_balancer	Integer	Definition: Specifies the maximum number of listeners that can be associated with a load balancer. Range: - 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	Definition: Specifies the maximum number of IP address groups that can be associated with a listener. Range: • If the value is greater than or equal to 0, it indicates the current quota. • -1 indicates that the quota is not limited.
pools_per_l7policy	Integer	Definition: Specifies the maximum number of backend server groups that can be associated with a forwarding policy. Range: • If the value is greater than or equal to 0, it indicates the current quota. • -1 indicates that the quota is not limited.
l7policies_per_listener	Integer	Definition: Specifies the maximum number of forwarding policies that can be associated with a listener. Range: • If the value is greater than or equal to 0, it indicates the current quota. • -1 indicates that the quota is not limited.
free_instance_members_per_pool	Integer	Definition: Specifies the maximum number of backend servers that can be added to a backend server group for free. Range: • If the value is greater than or equal to 0, it indicates the current quota. • -1 indicates that the quota is not limited.
free_instance_listeners_per_loadbalancer	Integer	Definition: Specifies the maximum number of listeners that can be associated with a load balancer for free. Range: • If the value is greater than or equal to 0, it indicates the current 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": "060576798a80d5762fafc01a9b5eecd7",
    "condition_per_policy": 10,
    "listeners_per_pool": 50,
    "listeners_per_loadbalancer": 50,
    "free_instance_members_per_pool": 50,
    "free_instance_listeners_per_loadbalancer": 10
  }
}
```

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 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 and used quotas of resources related to a load balancer.

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	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Table 5-8 Query Parameters

Parameter	Mandatory	Type	Description
quota_key	No	Array of strings	Definition: Specifies the quota type. Multiple values can be used for query in the format of <i>quota_key=xxx&quota_key=xxx</i> . Constraints: N/A Range: 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, l7policies_per_listener, free_instance_members_per_pool, or free_instance_listeners_per_loadbalancer Default value: N/A

Request Parameters

Table 5-9 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-10 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
quotas	Array of QuotaInfo objects	Definition: Specifies the resource quotas.

Table 5-11 QuotaInfo

Parameter	Type	Description
quota_key	String	Definition: Specifies the quota type. Range: 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, l7policies_per_listener, free_instance_members_per_pool, or free_instance_listeners_per_loadbalancer
quota_limit	Integer	Definition: Specifies the total quota. Range: • 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	Definition: Specifies the used quota. Range: greater than or equal to 0
unit	String	Definition: Specifies the quota unit. Range: count, indicating the number of resources

Example Requests

Querying the quota of a specific quota 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,  
    "unit" : "count"  
  } ]  
}
```

```
"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"
}, {
"quota_key" : "free_instance_members_per_pool",
"used" : 17,
"quota_limit" : 50,
"unit" : "count"
}, {
"quota_key" : "free_instance_listeners_per_loadbalancer",
"used" : 4,
"quota_limit" : 10,
"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.getStatusCode());
    System.out.println(e.getRequestId());
    System.out.println(e.getErrorCode());
    System.out.println(e.getErrorMsg());
}
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudskelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskelb.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	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Table 5-13 Query Parameters

Parameter	Mandatory	Type	Description
public_border_group	No	String	Definition: Specifies the public border group. Constraints: N/A Range: • center: public border group of the central site • Edge site name: public border group of an edge site Default value: N/A
loadbalancer_id	No	String	Definition: Specifies the ID of a load balancer to query the AZs it supports. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-14 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-15 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
availability_zones	Array<Array<AvailabilityZone>>	Definition: 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. Range: N/A

Table 5-16 AvailabilityZone

Parameter	Type	Description
code	String	Definition: Specifies the AZ code. Range: N/A
state	String	Definition: Specifies the AZ status. Range: ACTIVE.
protocol	Array of strings	Definition: Specifies the type of the flavors that is not sold out. Range: L4 indicates network load balancers are not sold out. L7 indicates application load balancers are not sold out.
public_border_group	String	Definition: Specifies the public border group. Range: - center: public border group of the central site - Edge site name: public border group of an edge site
category	Integer	Definition: Specifies the AZ category code. This parameter is used to identify the type of an edge AZ. Range: 0 (central AZs), 21 (HomeZones AZs), and 41 (edge AZs)

Parameter	Type	Description
spec_code	String	Definition: Specifies the code of the product in the edge AZ. The product code is used to query the price before purchasing a load balancer on the management console. Range: N/A

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",
    "spec_code": null,
    "category": 0
  }, {
    "state": "ACTIVE",
    "code": "az2",
    "protocol": [ "L4" ],
    "public_border_group": "center",
    "spec_code": null,
    "category": 0
  }, {
    "state": "ACTIVE",
    "code": "az3",
    "protocol": [ "L7" ],
    "public_border_group": "center",
    "spec_code": null,
    "category": 0
  }, {
    "state": "ACTIVE",
    "code": "homezone.az0",
    "protocol": [ "L4" ],
    "public_border_group": "homezone.azg",
    "spec_code": null,
    "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.getStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from 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.ElbcClientBuilder().
            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 available load balancer flavors in a specific region. You can specify these Layer 4 or Layer 7 flavors when creating a dedicated load balancer.

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	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Table 5-18 Query Parameters

Parameter	Mandatory	Type	Description
marker	No	String	Definition: Specifies the ID of the last record on the previous page. Constraints: • This parameter must be used together with limit. • If the parameter is not specified, only resources on the first page are queried. • This parameter cannot be left blank or set to an invalid ID. Range: N/A Default value: N/A
limit	No	Integer	Definition: Specifies the number of records returned on each page. Constraints: N/A Range: 0 to 2000 Default value: 2000

Parameter	Mandatory	Type	Description
page_reverse	No	Boolean	Definition: Specifies whether to use reverse query. Constraints: - This parameter must be used together with limit. - If page_reverse is set to true and you want to query the resources on the previous page, set the value of marker to the value of previous_marker. Range: true: Query resources on the previous page. false: Query resources on the next page. Default value: false
id	No	Array of strings	Definition: Specifies the flavor ID. Multiple IDs can be used for query in the format of <i>id=xxx&id=xxx</i>. Constraints: N/A Range: N/A Default value: N/A
name	No	Array of strings	Definition: Specifies the flavor name. Multiple names can be used for query in the format of <i>name=xxx&name=xxx</i>. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
type	No	Array of strings	Definition: Specifies the flavor type. Multiple types can be used for query in the format of <i>type=xxx&type=xxx</i>. Constraints: N/A Range: • L4 indicates a Layer 4 flavor and L7 indicates a Layer 7 flavor. • L4_elastic indicates the minimum elastic flavor at Layer 4 and L7_elastic indicates the minimum elastic flavor at Layer 7. • L4_elastic_max indicates the maximum elastic flavor at Layer 4 and L7_elastic_max indicates the maximum elastic flavor at Layer 7. Default value: N/A
shared	No	Boolean	Definition: Specifies whether to query the flavors available to all uses. Constraints: N/A Range: • true: Query the flavors available to all users. • false: Query the flavors only available to the current user. Default value: N/A

Parameter	Mandatory	Type	Description
public_border_group	No	Array of strings	Definition: Specifies the public border group. Multiple public border groups can be queried in the format of <i>public_border_group=xxx&public_border_group=xxx</i> . Constraints: N/A Range: • center: public border group of the central site • Edge site name: public border group of an edge site Default value: N/A
category	No	Array of integers	Definition: Specifies the AZ category code. This parameter is used to identify the type of an edge AZ. Multiple categories can be used for query in the format of <i>category=xxx&category=xxx</i> . Constraints: N/A Range: 0 (central AZs), 21 (HomeZones AZs), and 41 (edge AZs) Default value: N/A

Parameter	Mandatory	Type	Description
list_all	No	Boolean	Definition: Whether to query all the maximum elastic flavors of a specific user. Constraints: N/A Range: • true: All the maximum elastic flavors defined by l4_elastic_max and l7_elastic_max are returned. • false: Only the largest elastic flavors will be returned. For Layer 4 load balancers, the flavor with highest cps value is returned. If the cps values are the same, the flavor with highest bandwidth value is returned. For Layer 7 load balancers, the flavor with highest https_cps value is returned. If the https_cps values are the same, the flavor with highest qps value is returned. Default value: N/A
flavor_sold_out	No	Boolean	Specifies whether load balancers of this flavor are unavailable. Constraints: N/A • true indicates load balancers of this flavor are unavailable. • false indicates load balancers of this flavor are available. Default value: N/A

Request Parameters

Table 5-19 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-20 Response body parameters

Parameter	Type	Description
flavors	Array of Flavor objects	Definition: Specifies the flavor list.
page_info	PageInfo object	Definition: Specifies the pagination information.
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

Table 5-21 Flavor

Parameter	Type	Description
id	String	Definition: Specifies the flavor ID. Range: N/A
info	FlavorInfo object	Definition: Specifies the flavor metrics. Range: N/A

Parameter	Type	Description
name	String	Definition: Specifies the flavor name. Range: 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
shared	Boolean	Definition: Specifies whether the flavor is available to all users. Range: • true indicates that the flavor is available to all users. • false indicates that the flavor is available only to the current user.
project_id	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Range: The value can contain a maximum of 32 characters, including digits and lowercase letters.

Parameter	Type	Description
type	String	Definition: Specifies the flavor type. Range: • L4 indicates a Layer 4 flavor and L7 indicates a Layer 7 flavor. • L4_elastic indicates the minimum elastic flavor at Layer 4 and 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 and L7_elastic_max indicates the maximum elastic flavor at Layer 7.
flavor_sold_out	Boolean	Definition: Specifies whether load balancers of this flavor cannot be purchased. Range: • true: • false:
public_border_group	String	Definition: Specifies the public border group. Range: • center: public border group of the central site • Edge site name: public border group of an edge site
category	Integer	Definition: Specifies the AZ category code. This parameter is used to identify the type of an edge AZ. Range: 0 (central AZs), 21 (HomeZones AZs), and 41 (edge AZs)

Table 5-22 FlavorInfo

Parameter	Type	Description
connection	Integer	Definition: Specifies the maximum number of concurrent connections per second. Unit: count Range: N/A

Parameter	Type	Description
cps	Integer	Definition: Specifies the number of new connections per second. Unit: count Range: N/A
tls_connection	Integer	Definition: Specifies the maximum number of concurrent TLS connections per second. Unit: count Range: N/A
tls_cps	Integer	Definition: Specifies the maximum number of new TLS connections per second. Unit: count Range: N/A
qps	Integer	Definition: Specifies the number of queries per second (QPS). Unit: count. This parameter is available only for load balancers at Layer 7. Range: N/A
bandwidth	Integer	Definition: Specifies the bandwidth, in kbit/s. Range: N/A
lcu	Integer	Definition: Specifies the number of LCUs supported by the flavor. Unit: count Range: N/A NOTE An LCU measures the dimensions on which a dedicated load balancer routes the traffic. A higher value indicates better performance.
https_cps	Integer	Definition: Specifies the number of new HTTPS connections. This parameter is available only for load balancers at Layer 7. Unit: count Range: N/A

Table 5-23 PageInfo

Parameter	Type	Description
previous_marker	String	Definition: Specifies the ID of the first record in the pagination query result. If page_reverse is set to true , this parameter is used together to query resources on the previous page. Range: N/A
next_marker	String	Definition: Specifies the ID of the last record in the pagination query result. It is usually used to query resources on the next page. Range: N/A
current_count	Integer	Definition: Specifies the number of records returned on the current page. Range: N/A

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
}
}
```

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 ListFlavorsSolution {

    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();
        ListFlavorsRequest request = new ListFlavorsRequest();
        try {
            ListFlavorsResponse response = client.listFlavors(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 = ListFlavorsRequest()
        response = client.list_flavors(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.ListFlavorsRequest{}
response, err := client.ListFlavors(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](#).

5.4.2 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	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
flavor_id	Yes	String	Definition: Specifies the flavor ID. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-25 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-26 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

Parameter	Type	Description
flavor	Flavor object	Definition: Specifies the flavor.

Table 5-27 Flavor

Parameter	Type	Description
id	String	Definition: Specifies the flavor ID. Range: N/A
info	FlavorInfo object	Definition: Specifies the flavor metrics. Range: N/A
name	String	Definition: Specifies the flavor name. Range: 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

Parameter	Type	Description
shared	Boolean	Definition: Specifies whether the flavor is available to all users. Range: • true indicates that the flavor is available to all users. • false indicates that the flavor is available only to the current user.
project_id	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Range: The value can contain a maximum of 32 characters, including digits and lowercase letters.
type	String	Definition: Specifies the flavor type. Range: • L4 indicates a Layer 4 flavor and L7 indicates a Layer 7 flavor. • L4_elastic indicates the minimum elastic flavor at Layer 4 and 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 and L7_elastic_max indicates the maximum elastic flavor at Layer 7.
flavor_sold_out	Boolean	Definition: Specifies whether load balancers of this flavor cannot be purchased. Range: • true: • false:
public_border_group	String	Definition: Specifies the public border group. Range: • center: public border group of the central site • Edge site name: public border group of an edge site

Parameter	Type	Description
category	Integer	Definition: Specifies the AZ category code. This parameter is used to identify the type of an edge AZ. Range: 0 (central AZs), 21 (HomeZones AZs), and 41 (edge AZs)

Table 5-28 FlavorInfo

Parameter	Type	Description
connection	Integer	Definition: Specifies the maximum number of concurrent connections per second. Unit: count Range: N/A
cps	Integer	Definition: Specifies the number of new connections per second. Unit: count Range: N/A
tls_connection	Integer	Definition: Specifies the maximum number of concurrent TLS connections per second. Unit: count Range: N/A
tls_cps	Integer	Definition: Specifies the maximum number of new TLS connections per second. Unit: count Range: N/A
qps	Integer	Definition: Specifies the number of queries per second (QPS). Unit: count. This parameter is available only for load balancers at Layer 7. Range: N/A
bandwidth	Integer	Definition: Specifies the bandwidth, in kbit/s. Range: N/A
lcu	Integer	Definition: Specifies the number of LCUs supported by the flavor. Unit: count Range: N/A NOTE An LCU measures the dimensions on which a dedicated load balancer routes the traffic. A higher value indicates better performance.

Parameter	Type	Description
https_cps	Integer	Definition: Specifies the number of new HTTPS connections. This parameter is available only for load balancers at Layer 7. Unit: count Range: N/A

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" : "8d53f081ea2444aa95e2bfa942ef6ee",
    "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.getenv("CLOUD_SDK_AK")
    sk = os.getenv("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 Layer 7 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 does 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	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Table 5-30 Query Parameters

Parameter	Mandatory	Type	Description
l7_flavor_id	No	String	Definition: 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. Constraints: This parameter can only be used for creating a dedicated load balancer with a Layer 7 flavor or changing the Layer 7 flavor of a dedicated load balancer Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
ip_target_enable	No	Boolean	Definition: Whether to enable IP as a Backend. Constraints: This parameter can only be used 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. Range: • 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 will be calculated. • If this parameter is not passed, IP as a Backend is disabled. Default value: false
ip_version	No	Integer	Definition: Specifies the IP address version of the load balancer. The value can be 4 or 6. Constraints: This parameter can be used for creating a load balancer. Range: • 4: The number of reserved IPv4 addresses required for creating a load balancer will be calculated. • 6: The number of reserved IPv6 addresses required for creating a load balancer will be calculated. Default value: N/A

Parameter	Mandatory	Type	Description
loadbalancer_id	No	String	Definition: 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 Layer 7 listener to a load balancer will be calculated. Constraints: This parameter can be used for 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 Layer 7 listener to a load balancer. Range: N/A Default value: N/A
availability_zone_id	No	Array of strings	Definition: Calculates the number of reserved IP addresses required for creating a load balancer in the AZs specified by availability_zone_id. Constraints: • This parameter can only be used for creating a load balancer. • This parameter is invalid if loadbalancer_id is specified. Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
scene	No	String	Definition: Calculates the number of IP addresses required for upgrading a shared load balancer to a dedicated load balancer. Constraints: • This parameter can only be used for upgrading a shared load balancer to a dedicated load balancer. • Both this parameter and loadbalancer_id must be specified. Range: UPGRADE (upgrading a shared load balancer to a dedicated load balancer) Default value: N/A
nat64_enable	No	Boolean	Definition: 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. Constraints: • This parameter can only be used for calculating the number of reserved IP addresses required for enabling nat64_enable for the listeners of a load balancer. Range: • 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	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-32 Response body parameters

Parameter	Type	Description
preoccupy_ip	PreoccupypIp object	Definition: Specifies reserved IP address.
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

Table 5-33 PreoccupypIp

Parameter	Type	Description
total	Integer	Definition: Specifies the number of preoccupied IP addresses. Range: an integer no less than 0

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=tr
ue

{
  "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 huaweicloudskelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskelb.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 huaweicloudskelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskelb.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 huaweicloudskelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskelb.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.ElClientBuilder().
            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.ElClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
```



```
Build()

request := &model.CountPreoccupypIpNumRequest{}
response, err := client.CountPreoccupypIpNum(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.CountPreoccupypIpNumRequest{}
    response, err := client.CountPreoccupypIpNum(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 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 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.
- 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 an existing 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	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-35 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-36 Request body parameters

Parameter	Mandatory	Type	Description
loadbalancer	Yes	CreateLoadBalancerOption object	Definition: Specifies the parameters for creating a load balancer. Constraints: N/A

Table 5-37 CreateLoadBalancerOption

Parameter	Mandatory	Type	Description
project_id	No	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A NOTE This parameter is invalid. The project ID in the URL is used.
name	No	String	Definition: Specifies the load balancer name. Constraints: N/A Range: The value can contain a maximum of 255 Unicode characters, including letters and more. It can be left blank. Default value: N/A

Parameter	Mandatory	Type	Description
description	No	String	Definition: Provides supplementary information about the load balancer. Constraints: N/A Range: The value can contain a maximum of 255 Unicode characters, including letters and more. It can be left blank. Default value: N/A
vip_address	No	String	Definition: Specifies the private IPv4 address of 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. Constraints: • 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. Range: The IP address must be in [0-255].[0-255].[0-255].[0-255] format, for example, 192.168.1.1. Default value: N/A

Parameter	Mandatory	Type	Description
<code>vip_subnet_cidr_id</code>	No	String	Definition: Specifies the ID of the IPv4 subnet where the load balancer is located. This subnet is also called the frontend subnet. Constraints: • This parameter is mandatory if you need to create a load balancer with a private IPv4 address. You can query parameter neutron_subnet_id in the response by calling the VPC API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets). • 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. Range: The ID must be in UUID format and can contain up to 36 characters. Default value: N/A

Parameter	Mandatory	Type	Description
ipv6_vip_virsubnet_id	No	String	Definition: Specifies the ID of the IPv6 subnet where the load balancer is located. This subnet is also called the frontend subnet. Constraints: • This parameter is mandatory if you need to create a load balancer with a private IPv6 address. You can query parameter neutron_network_id in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets). • 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. Range: The ID must be in UUID format and can contain up to 36 characters. Default value: N/A
provider	No	String	Definition: Specifies the provider of the load balancer. Constraints: N/A Range: The value can only be vlb and does not need to be specified. Default value: vlb

Parameter	Mandatory	Type	Description
l4_flavor_id	No	String	Definition: Specifies the ID of a flavor at Layer 4. Constraints: • 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 flavors and will be billed by the flavor you select. • If the flavor type is L4_elastic_max, the load balancer uses the elastic flavors and will be billed by how many LCUs you use. Range: The ID must be in UUID format and can contain up to 36 characters. Default value: N/A

Parameter	Mandatory	Type	Description
<code>l7_flavor_id</code>	No	String	Definition: Specifies the ID of a flavor at Layer 7. Constraints: • You can query parameter id in the response by calling the API (GET <code>https://{ELB_Endpoint}/v3/{project_id}/elb/flavors?type=L7</code>). • 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 flavors and will be billed by the flavor you select. • If the flavor type is L7_elastic_max, the load balancer uses the elastic flavors and will be billed by how many LCUs you use. Range: The ID must be in UUID format and can contain up to 36 characters. Default value: N/A
<code>guaranteed</code>	No	Boolean	Definition: Specifies whether to create a shared or dedicated load balancer. Currently, the value can only be true. If the value is set to false, 400 Bad Request will be returned. Range: • true: Dedicated load balancers will be created. • false: Shared load balancers will be created. Default value: true

Parameter	Mandatory	Type	Description
vpc_id	No	String	Definition: Specifies the ID of the VPC where the load balancer is located. Constraints: - You can query parameter id in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/vpcs). 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. Range: The ID must be in UUID format and can contain up to 36 characters. Default value: N/A
availability_zone_list	Yes	Array of strings	Definition: Specifies the list of AZs where the load balancers are 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. Constraints: N/A Range: N/A Default value: N/A NOTE If disaster recovery is required, you are advised to select multiple AZs.

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Definition: Specifies the ID of the enterprise project. If no enterprise project ID is specified during resource creation, 0 is returned, indicating that the resource belongs to the default enterprise project. Constraints: The enterprise project ID cannot be "", 0, or an enterprise project ID that does not exist. Range: N/A Default value: 0
tags	No	Array of Tag objects	Definition: Specifies the tags added to the load balancer. Example: "tags": [{"key": "my_tag", "value": "my_tag_value"}] Constraints: N/A
admin_state_up	No	Boolean	Definition: Specifies whether the load balancer is enabled. Constraints: N/A Range: • true: enabled • false: disabled Default value: true
billing_info	No	String	Definition: Provides resource billing information. Constraints: N/A Range: • If the value is left blank, the resource is billed on a pay-per-use basis. Default value: N/A This parameter is unsupported. Please do not use it.

Parameter	Mandatory	Type	Description
ipv6_bandwidth	No	BandwidthRef object	Definition: Specifies the ID of the bandwidth. Constraints: • This parameter is available only when you create or update a load balancer with a public address. • If you bind a new EIP to the load balancer and specify a shared bandwidth, this EIP will be added to the shared bandwidth.
publicip_ids	No	Array of strings	Definition: Specifies the IDs of the EIPs bound to the load balancer. Constraints: • Only the first EIP in the array will be bound.
publicip	No	CreateLoadBalancerPublicIpOption object	Definition: Specifies the request parameters for binding a new EIP to the load balancer. Constraints: N/A

Parameter	Mandatory	Type	Description
elb_virsubnet_ids	No	Array of strings	Definition: (OpenStack Neutron API) Specifies the network IDs of backend subnets where the load balancers work. A load balancer uses IP addresses in the backend subnet to communicate with backend servers (such as in health check and FullNAT scenarios). 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). Constraints: • 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 to assign IP addresses. • If this parameter is not specified, the network IDs will be used based on the following rules: – If IPv6 is enabled for a load balancer, the network IDs of subnets specified in ipv6_vip_virsubnet_id will be used. – If IPv6 is not enabled for a load balancer, the network IDs of subnets specified in

Parameter	Mandatory	Type	Description
			vip_subnet_cidr_id will be used. – If a load balancer only works on the public network, any subnet in the VPC where the load balancer is deployed will be used. The subnet with the most available IP addresses is preferred. • 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 only allowing certain IP addresses. • You are advised to use a dedicated subnet with sufficient IP addresses for easier O&M. Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
ip_target_enable	No	Boolean	Definition: Specifies whether to add backend servers that are not in the load balancer's VPC. 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. Constraints: • This function cannot be disabled once it is enabled. • If you want to enable IP as a Backend for a load balancer in a shared VPC, ensure that a VPC peering connection has been created to connect the VPCs. Otherwise, the communication will fail. • This function is supported only by dedicated load balancers. Range: • true: This option will be enabled. • false: This option will be disabled. Default value: false

Parameter	Mandatory	Type	Description
deletion_protection_enable	No	Boolean	Definition: Specifies whether to enable deletion protection for the load balancer. Constraints: Before deleting a load balancer, you need to disable deletion protection first. Range: • false: This option will not be enabled. • true: This option will be enabled. Default value: false
prepaid_options	No	PrepaidCreateOption object	Definition: Specifies the prepaid billing configuration for creating a load balancer. If this structure is passed, a prepaid load balancer is created. Constraints: N/A This parameter is unsupported. Please do not use it.

Parameter	Mandatory	Type	Description
autoscaling	No	CreateLoadbalancerAutoscalingOption object	Definition: Specifies information about elastic scaling. If elastic scaling is enabled, the load balancer flavors can be automatically adjusted based on incoming traffic. Constraints: - This parameter is only available for whitelisted users. - 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. NOTE 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 flavors will be created and you will be billed for the minimum flavors.
waf_failure_action	No	String	Definition: Specifies traffic distributing policies when the WAF is faulty. Constraints: This parameter takes effect only when WAF is enabled for the load balancer. Range: discard: Traffic will not be distributed. forward: Traffic will be distributed to the backend servers. Default value: forward

Parameter	Mandatory	Type	Description
protection_status	No	String	Definition: 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. Constraints: You can call APIs to modify resource attributes, such as resource tags. This improves user experience on the console, for example, preventing accidental modification. Range: • nonProtection: The resource is not protected. • consoleProtection: Modification is not allowed on the console. Default value: nonProtection
protection_reason	No	String	Definition: Specifies why modification protection is enabled. Constraints: This parameter is valid only when protection_status is set to consoleProtection. Range: The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>). Default value: N/A

Parameter	Mandatory	Type	Description
charge_mode	No	String	Definition: Specifies the charge mode of the load balancer. 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. Range: • flavor: billed by the fixed flavor you select. • lcu: billed by how many LCUs you have used. Default value: • 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	Definition: Specifies the IPv6 address used by the load balancer. Constraints: • 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. Range: N/A Default value: N/A

Table 5-38 Tag

Parameter	Mandatory	Type	Description
key	No	String	Definition: Specifies the tag key. Range: N/A
value	No	String	Definition: Specifies the tag value. Range: N/A

Table 5-39 BandwidthRef

Parameter	Mandatory	Type	Description
id	Yes	String	Definition: Specifies the ID of the shared bandwidth. Constraints: N/A Range: N/A Default value: N/A

Table 5-40 CreateLoadBalancerPublicIpOption

Parameter	Mandatory	Type	Description
ip_version	No	Integer	Definition: Specifies the IP address version. Constraints: N/A Range: • 4: IPv4 addresses • 6: IPv6 addresses Default value: 4
network_type	Yes	String	Definition: Specifies the EIP type. The default value is 5_bgp . For more information, see the API for assigning an EIP in the <i>Virtual Private Cloud API Reference</i> . Range: 5_bgp Default value: 5_bgp

Parameter	Mandatory	Type	Description
billing_info	No	String	Definition: Provides billing information about the EIP. Constraints: If the value is left blank, the resource is billed on a pay-per-use basis. Range: N/A Default value: N/A This parameter is unsupported. Please do not use it.
description	No	String	Definition: Provides supplementary information about the EIP. Constraints: N/A Range: N/A Default value: N/A
bandwidth	Yes	CreateLoadBalancerBandwidthOption object	Definition: Provides supplementary information about the bandwidth. Constraints: N/A

Table 5-41 CreateLoadBalancerBandwidthOption

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

Parameter	Mandatory	Type	Description
size	No	Integer	Definition: Specifies the bandwidth size. Constraints: • This parameter is mandatory if id is set to null. • The minimum increment for bandwidth adjustment varies by bandwidth range. The details are as follows: – 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. Range: The default value ranges from 1 Mbit/s to 2,000 Mbit/s, which may vary by region and can be viewed on the management console. Default value: N/A
charge_mode	No	String	Definition: Specifies how the bandwidth used by the EIP is billed. Constraints: This parameter is mandatory if id is set to null. Range: • bandwidth: billed by bandwidth • traffic: billed by traffic Default value: N/A

Parameter	Mandatory	Type	Description
share_type	No	String	Definition: Specifies the bandwidth type. Constraints: • 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. Range: • PER: dedicated bandwidths • WHOLE: shared bandwidths Default value: N/A
billing_info	No	String	Definition: Provides resource billing information. Constraints: N/A Range: N/A Default value: N/A This parameter is unsupported. Please do not use it.
id	No	String	Definition: Specifies the ID of the shared bandwidth. An existing shared bandwidth is used. Constraints: The ID must be an existing shared bandwidth ID. There is no need to specify this parameter if the billing mode is yearly/monthly. This parameter will be ignored if it is left blank. Range: N/A Default value: N/A

Table 5-42 PrepaidCreateOption

Parameter	Mandatory	Type	Description
period_type	Yes	String	Definition: Specifies the subscription period type. Constraints: N/A Range: • month: monthly subscription • year: yearly subscription Default value: N/A
period_num	No	Integer	Definition: Specifies the number of subscription periods. Constraints: N/A Range: • 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. Default value: N/A
auto_renew	No	Boolean	Definition: Specifies whether to enable automatic renewal. Constraints: N/A Range: • true: Enable automatic renewal. • false (default): Disable automatic renewal. Default value: N/A

Parameter	Mandatory	Type	Description
auto_pay	No	Boolean	Definition: Specifies whether an order is automatically paid using your account balance without manual operations. Constraints: If you use the automatic payment mode, only your account balance can be used. If you want to use a voucher, do not use the automatic payment mode, and select the voucher for the payment in the Billing Center. Range: • true: The order will be automatically paid. • false: The order will not be automatically paid. Default value: N/A

Table 5-43 CreateLoadbalancerAutoscalingOption

Parameter	Mandatory	Type	Description
enable	Yes	Boolean	Definition: Specifies whether to enable elastic scaling for the load balancer. Constraints: N/A Range: • true: This option will be enabled. • false: This option will be disabled. Default value: N/A
min_l7_flavor_id	No	String	Definition: Specifies the ID of the minimum elastic flavor at Layer 7. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 201

Table 5-44 Response body parameters

Parameter	Type	Description
loadbalancer	LoadBalancer object	Definition: Specifies the load balancer.
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

Table 5-45 LoadBalancer

Parameter	Type	Description
id	String	Definition: Specifies the load balancer ID. Range: N/A
description	String	Definition: Provides supplementary information about the load balancer. Range: N/A
provisioning_status	String	Definition: Specifies the provisioning status of the load balancer. Range: • ACTIVE: in use • PENDING_DELETE: deleting
admin_state_up	Boolean	Definition: Specifies whether the load balancer is enabled. Range: • true: enabled • false: disabled
provider	String	Definition: Specifies the provider of the load balancer. The value is fixed to vlb . Range: N/A
pools	Array of PoolRef objects	Definition: Lists the IDs of backend server groups associated with the load balancer.
listeners	Array of ListenerRef objects	Definition: Lists the IDs of listeners associated with the load balancer.

Parameter	Type	Description
operating_status	String	Definition: Specifies the operating status of the load balancer. Range: • ONLINE: The load balancer is online. • FROZEN: The load balancer is frozen.
name	String	Definition: Specifies the load balancer name. Range: N/A
project_id	String	Definition: Specifies the ID of the project where the load balancer is used. Range: N/A
vip_subnet_cidr_id	String	Definition: Specifies the ID of the IPv4 subnet where the load balancer is located. This subnet is also called the frontend subnet. Range: N/A
vip_address	String	Definition: Specifies the private IPv4 address of the load balancer. Range: N/A
vip_port_id	String	Definition: Specifies the ID of the port bound to the private IPv4 address of the load balancer. Range: N/A
tags	Array of Tag objects	Definition: Specifies the tags added to the load balancer.
created_at	String	Definition: Specifies the time when the load balancer was created. Range: The value must be in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> .
updated_at	String	Definition: Specifies the time when the load balancer was updated. Range: The value must be in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> .

Parameter	Type	Description
guaranteed	Boolean	Definition: Specifies whether the load balancer is a dedicated load balancer. Range: • false: The load balancer is a shared load balancer. • true: The load balancer is a dedicated load balancer.
vpc_id	String	Definition: Specifies the ID of the VPC where the load balancer is located. Range: N/A
eips	Array of EipInfo objects	Definition: Specifies the EIP bound to the load balancer. NOTE This parameter has the same meaning as publicips .
ipv6_vip_address	String	Definition: Specifies the IPv6 address of the load balancer. Range: N/A
ipv6_vip_virsubnet_id	String	Definition: Specifies the ID of the IPv6 subnet where the load balancer is located. This subnet is also called the frontend subnet. Range: N/A
ipv6_vip_port_id	String	Definition: Specifies the ID of the port bound to the IPv6 address of the load balancer. Range: N/A
availability_zone_list	Array of strings	Definition: Specifies the list of AZs where the load balancers are created. Range: N/A
enterprise_project_id	String	Definition: Specifies the ID of the enterprise project. Range: • 0: The resource belongs to the default enterprise project. • A string in UUID format indicates a non-default enterprise project.

Parameter	Type	Description
billing_info	String	Definition: Provides resource billing information. Range: If the value is left blank, the resource is billed on a pay-per-use basis. This parameter is unsupported. Please do not use it.
l4_flavor_id	String	Definition: Specifies the ID of a flavor at Layer 4. If the current load balancer is an elastic flavor instance, this parameter defines the maximum elastic flavor at Layer 4. Range: N/A
l4_scale_flavor_id	String	Definition: Specifies the ID of an elastic flavor at Layer 4. Range: N/A NOTE This parameter has been discarded. Do not use it.
l7_flavor_id	String	Definition: Specifies the ID of a flavor at Layer 7. If the current load balancer is an elastic flavor instance, this parameter defines the maximum elastic flavor at Layer 7. Range: N/A
l7_scale_flavor_id	String	Definition: Specifies the ID of an elastic flavor at Layer 7. Range: N/A NOTE This parameter has been discarded. Do not use it.
gw_flavor_id	String	Definition: Specifies the flavor ID of the gateway load balancer. Range: N/A This parameter is unsupported. Please do not use it.

Parameter	Type	Description
loadbalancer_type	String	Definition: Specifies the load balancer type. Range: • gateway: gateway load balancers • null: other types of load balancers This parameter is unsupported. Please do not use it.
publicips	Array of PublicIpInfo objects	Definition: Specifies the EIP bound to the load balancer. NOTE This parameter has the same meaning as eips .
global_eips	Array of GlobalEipInfo objects	Definition: Specifies the global EIP bound to the load balancer.
elb_virsubnet_ids	Array of strings	Definition: Specifies the network IDs of subnets on the downstream plane. Range: N/A
elb_virsubnet_type	String	Definition: Specifies the type of the subnet on the downstream plane. Range: • ipv4: IPv4 subnets • dualstack: subnets that support IPv4/IPv6 dual stack
ip_target_enable	Boolean	Definition: Specifies whether to add backend servers that are not in the load balancer's VPC. 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. Range: • true: This option will be enabled. • false: This option will be disabled.

Parameter	Type	Description
frozen_scene	String	Definition: Specifies the scenario where the load balancer is frozen. If there are multiple scenarios, separate them with commas (.). Range: • 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. • AREAR: The load balancer is frozen due to arrears.
deletion_protection_enable	Boolean	Definition: Specifies whether to enable deletion protection. This parameter is returned only when the deletion protection is enabled in the current region. Range: • false: This option will be disabled. • true: This option will be enabled.
autoscaling	AutoscalingRef object	Definition: Specifies information about elastic scaling. If elastic scaling is enabled, the load balancer flavors can be automatically adjusted based on incoming traffic. NOTE 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 flavors will be created and you will be billed for the minimum flavors.
public_border_group	String	Definition: Specifies the public border group. Range: • center: public border group of the central site • Edge site name: public border group of an edge site

Parameter	Type	Description
charge_mode	String	Definition: Specifies the charge mode of the load balancer. Range: • flavor: billed by the fixed flavor you select. • lcu: billed by how many LCUs you have used. • Null: If it is a shared load balancer, it is free. If it is a dedicated load balancer, it will be billed by the fixed flavor you select. This parameter is unsupported. Please do not use it.
service_lb_mode	String	Definition: Specifies load balancer mode. Range: • lb: Cross-tenant access is not supported. • ep: Cross-tenant access is supported. This parameter is unsupported. Please do not use it.
instance_type	String	Definition: Specifies the internal service to which the load balancer belongs. Range: N/A This parameter is unsupported. Please do not use it.
instance_id	String	Definition: Specifies the ID of the instance with which the load balancer is associated. Range: N/A This parameter is unsupported. Please do not use it.
proxy_protocol_extensions	Array of ProxyProtocolExtension objects	Definition: Specifies the proxy protocol extension. This parameter is unsupported. Please do not use it.

Parameter	Type	Description
waf_failure_action	String	Definition: Specifies traffic distributing policies when the WAF is faulty. Range: discard indicates traffic will not be distributed. forward indicates traffic will be distributed to the default backend servers.
protection_status	String	Definition: Specifies the protection status. Range: • nonProtection: The resource is not protected. • consoleProtection: Modification is not allowed on the console.
protection_reason	String	Definition: Specifies why modification protection is enabled. Range: The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).
log_group_id	String	Definition: Specifies the ID of the log group that is associated with the load balancer. Range: N/A
log_topic_id	String	Definition: Specifies the ID of the log topic that is associated with the load balancer. Range: N/A
custom_qos_limit	CustomQosLimit object	Definition: Specifies the rate limit information of the ELB flavors. Range: N/A This parameter is unsupported. Please do not use it.

Table 5-46 PoolRef

Parameter	Type	Description
id	String	Definition: Specifies the backend server group ID. Range: N/A

Table 5-47 ListenerRef

Parameter	Type	Description
id	String	Definition: Specifies the listener ID. Range: N/A

Table 5-48 Tag

Parameter	Type	Description
key	String	Definition: Specifies the tag key. Range: N/A
value	String	Definition: Specifies the tag value. Range: N/A

Table 5-49 EipInfo

Parameter	Type	Description
eip_id	String	Definition: Specifies the EIP ID. Range: N/A
eip_address	String	Definition: Specifies the EIP. Range: N/A
ip_version	Integer	Definition: Specifies the IP address version. Range: • 4: IPv4 addresses • 6: IPv6 addresses

Table 5-50 PublicIpInfo

Parameter	Type	Description
publicip_id	String	Definition: Specifies the EIP ID. Range: N/A
publicip_address	String	Definition: Specifies the EIP. Range: N/A

Parameter	Type	Description
ip_version	Integer	Definition: Specifies the IP address version. Range: • 4: IPv4 address • 6: IPv6 address

Table 5-51 GlobalEipInfo

Parameter	Type	Description
global_eip_id	String	Definition: Specifies the ID of the global EIP. Range: N/A
global_eip_addresses	String	Definition: Specifies the global EIP. Range: N/A
ip_version	Integer	Definition: Specifies the IP address version. Range: • 4: IPv4 addresses • 6: IPv6 addresses

Table 5-52 AutoscalingRef

Parameter	Type	Description
enable	Boolean	Definition: Specifies whether to enable elastic scaling for the load balancer. Range: • true: This option will be enabled. • false: This option will be disabled.
min_l7_flavor_id	String	Definition: Specifies the ID of the minimum elastic flavor at Layer 7. Range: N/A

Table 5-53 ProxyProtocolExtension

Parameter	Type	Description
vip_address	String	Definition: Specifies the IPv4 address. Constraints: N/A Range: N/A Default value: N/A
ipv6_vip_address	String	Definition: Specifies the IPv6 address. Constraints: N/A Range: N/A Default value: N/A
extension	Extension object	Definition: Specifies the proxy protocol extension. Constraints: N/A

Table 5-54 Extension

Parameter	Type	Description
ep_id	String	Definition: Specifies the VPC endpoint ID. Constraints: N/A Range: N/A Default value: N/A
ep_service_id	String	Definition: Specifies the VPC endpoint service ID. Constraints: N/A Range: N/A Default value: N/A

Table 5-55 CustomQosLimit

Parameter	Type	Description
l4	L4Limit object	Definition: Specifies the rate limit information of the ELB flavors at Layer 4.
l7	L7Limit object	Definition: Specifies the rate limit information of the ELB flavors at Layer 7.

Table 5-56 L4Limit

Parameter	Type	Description
connection	Integer	Definition: Specifies the maximum number of concurrent connections at Layer 4. Range: N/A
cps	Integer	Definition: Specifies the maximum number of new connections at Layer 4. Range: N/A

Table 5-57 L7Limit

Parameter	Type	Description
connection	Integer	Definition: Specifies the maximum number of concurrent connections at Layer 7. Range: N/A
cps	Integer	Definition: Specifies the maximum number of new connections at Layer 7. Range: N/A

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

Successful request.

```
{  
  "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": "tag_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.setName("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.setName("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();  
        }  
    }  
}
```



```
        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 huaweicloudskelb.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.ElClientBuilder().
        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	Successful request.

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 in batches:

- **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.
- 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 an existing 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 a load balancer.

Calling Method

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

URI

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

Table 5-58 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-59 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-60 Request body parameters

Parameter	Mandatory	Type	Description
loadbalancer	Yes	BatchCreateLoadBalancerOption object	Specifies the load balancer. Constraints: N/A

Table 5-61 BatchCreateLoadBalancerOption

Parameter	Mandatory	Type	Description
id	No	String	Definition: Specifies the load balancer ID. Constraints: N/A Range: N/A Default value: N/A This parameter is unsupported. Please do not use it.
ids	No	Array of strings	Definition: Specifies the IDs of the load balancers created in batches. Constraints: N/A Range: N/A Default value: N/A This parameter is unsupported. Please do not use it.

Parameter	Mandatory	Type	Description
project_id	No	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
number	No	Integer	Definition: Specifies the number of load balancers to be created. Constraints: N/A Range: 1 to 10 Default value: 1
name	No	String	Definition: Specifies the load balancer name. • 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. Constraints: N/A Range: N/A Default value: N/A
description	No	String	Definition: Provides supplementary information about the load balancers. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
vip_address	No	String	Definition: Specifies the private IPv4 address of 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. Constraints: • 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. Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
<code>vip_subnet_cidr_id</code>	No	String	Definition: 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). Constraints: • 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. Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
ipv6_vip_virsubnet_id	No	String	Definition: 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). Constraints: • 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. Range: N/A Default value: N/A
provider	No	String	Definition: Specifies the provider of the load balancer. The value is fixed to vlb. Constraints: This parameter cannot be specified when shared load balancers are created in batches. Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
l4_flavor_id	No	String	Definition: Specifies the ID of a flavor at Layer 4. You can query parameter id in the response by calling the API (GET https://{ELB_Endpoint}/v3/{project_id}/elb/flavors?type=L4). Constraints: • 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 flavors and will be billed by the flavor you select. • If the flavor type is L4_elastic_max, the load balancer uses the elastic flavors and will be billed by how many LCUs you use. • This parameter cannot be specified when shared load balancers are created in batches. Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
<code>l7_flavor_id</code>	No	String	Definition: Specifies the ID of a flavor at Layer 7. You can query parameter id in the response by calling the API (GET <code>https://{ELB_Endpoint}/v3/{project_id}/elb/flavors?type=L7</code>). Constraints: • 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 flavors and will be billed by the flavor you select. • If the flavor type is L7_elastic_max, the load balancer uses the elastic flavors and will be billed by how many LCUs you use. • This parameter cannot be specified when shared load balancers are created in batches. Range: N/A Default value: N/A
<code>guaranteed</code>	No	Boolean	Definition: Specifies whether to create dedicated or shared load balancers. Constraints: N/A Range: • true: Dedicated load balancers will be created. • false: Shared load balancers will be created. Default value: true

Parameter	Mandatory	Type	Description
vpc_id	No	String	Definition: Specifies the ID of the VPC where the load balancer is located. You can query parameter id in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/vpcs). Constraints: • 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. Range: N/A Default value: N/A
availability_zone_list	Yes	Array of strings	Definition: Specifies the list of AZs where the load balancers 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. Constraints: • This parameter cannot be specified when shared load balancers are created in batches. Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Definition: Specifies the ID of the enterprise project. If no enterprise project ID is specified during resource creation, 0 is returned, indicating that the resource belongs to the default enterprise project. Constraints: The enterprise project ID cannot be "", 0, or an enterprise project ID that does not exist. Range: N/A Default value: 0
tags	No	Array of Tag objects	Definition: Specifies the tags added to the load balancer. Example: "tags": [{"key": "my_tag", "value": "my_tag_value"}] Constraints: N/A
admin_state_up	No	Boolean	Definition: Specifies whether the load balancer is enabled. Constraints: N/A Range: • true: enabled • false: disabled Default value: true
ipv6_bandwidth	No	BandwidthRef object	Definition: Specifies the ID of the bandwidth. Constraints: • This parameter is available only when you create or update a load balancer with a public address. • If you bind a new EIP to the load balancer and specify a shared bandwidth, this EIP will be added to the shared bandwidth.

Parameter	Mandatory	Type	Description
bandwidth	No	BandwidthRef object	Definition: Specifies the ID of the bandwidth. Constraints: • This parameter is available only when you create or update a load balancer with a public address. • If you bind a new EIP to the load balancer and specify a shared bandwidth, this EIP will be added to the shared bandwidth.
publicip_ids	No	Array of strings	Definition: 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. Constraints: N/A Range: N/A Default value: N/A
publicip	No	CreateLoadBalancerPublicIpOption object	Definition: Specifies the request parameters for binding a new EIP to the load balancer. Constraints: N/A

Parameter	Mandatory	Type	Description
elb_virsubnet_ids	No	Array of strings	Definition: Specifies the network 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 network IDs will be used based on the following rules: • If IPv6 is enabled for a load balancer, the network IDs of subnets specified in ipv6_vip_virsubnet_id will be used. • If IPv6 is not enabled for a load balancer, the network IDs of subnets specified in vip_subnet_cidr_id will be used. • If a load balancer only works on the public network, any subnet in the VPC where the load balancer is deployed will be used. The subnet with the most available IP addresses is 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. Constraints: The subnets must be in the VPC where the load balancer works. Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
ip_target_enable	No	Boolean	Definition: Specifies whether to add backend servers that are not in the load balancer's VPC. 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. Constraints: • This function cannot be disabled once it is enabled. • If you want to enable IP as a Backend for a load balancer in a shared VPC, ensure that a VPC peering connection has been created to connect the VPCs. Otherwise, the communication will fail. • This function is supported only by dedicated load balancers. Range: • true: This option will be enabled. • false: This option will be disabled. Default value: false

Parameter	Mandatory	Type	Description
deletion_protection_enable	No	Boolean	Definition: Specifies whether to enable deletion protection. Constraints: This parameter cannot be specified when shared load balancers are created in batches. Range: false (disable this option) or true (enable this option). Default value: false NOTE Disable deletion protection or removal protection for your resources before deregistering your account.
autoscaling	No	CreateLoadBalancerAutoScalingOption object	Definition: Specifies information about elastic scaling. If elastic scaling is enabled, the load balancer flavors can be automatically adjusted based on incoming traffic. Constraints: • This parameter is only available for whitelisted users. • 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. NOTE 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 flavors will be created and you will be billed for the minimum flavors.

Parameter	Mandatory	Type	Description
waf_failure_action	No	String	Definition: Specifies traffic distributing policies when the WAF is faulty. Constraints: This parameter takes effect only when WAF is enabled for the load balancer. Range: • discard: Traffic will not be distributed. • forward: Traffic will be distributed to the backend servers. Default value: forward
protection_status	No	String	Definition: Specifies the protection status. Constraints: N/A Range: • nonProtection: The resource is not protected. • consoleProtection: Modification is not allowed on the console. Default value: nonProtection
protection_reason	No	String	Definition: Specifies why modification protection is enabled. Constraints: This parameter is valid only when protection_status is set to consoleProtection. Range: The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>). Default value: N/A

Parameter	Mandatory	Type	Description
ipv6_vip_address	No	String	Definition: Specifies the IPv6 address of the load balancer. Constraints: - 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. Range: N/A Default value: N/A

Table 5-62 Tag

Parameter	Mandatory	Type	Description
key	No	String	Definition: Specifies the tag key. Range: N/A
value	No	String	Definition: Specifies the tag value. Range: N/A

Table 5-63 BandwidthRef

Parameter	Mandatory	Type	Description
id	Yes	String	Definition: Specifies the ID of the shared bandwidth. Constraints: N/A Range: N/A Default value: N/A

Table 5-64 CreateLoadBalancerPublicIpOption

Parameter	Mandatory	Type	Description
ip_version	No	Integer	Definition: Specifies the IP address version. Constraints: N/A Range: • 4: IPv4 addresses • 6: IPv6 addresses Default value: 4
network_type	Yes	String	Definition: Specifies the EIP type. The default value is 5_bgp . For more information, see the API for assigning an EIP in the <i>Virtual Private Cloud API Reference</i> . Range: 5_bgp Default value: 5_bgp
billing_info	No	String	Definition: Provides billing information about the EIP. Constraints: • If the value is left blank, the resource is billed on a pay-per-use basis. Range: N/A Default value: N/A This parameter is unsupported. Please do not use it.
description	No	String	Definition: Provides supplementary information about the EIP. Constraints: N/A Range: N/A Default value: N/A
bandwidth	Yes	CreateLoadBalancerBandwidthOption object	Definition: Provides supplementary information about the bandwidth. Constraints: N/A

Table 5-65 CreateLoadBalancerBandwidthOption

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

Parameter	Mandatory	Type	Description
charge_mode	No	String	Definition: Specifies how the bandwidth used by the EIP is billed. Constraints: This parameter is mandatory if id is set to null . Range: • bandwidth: billed by bandwidth • traffic: billed by traffic Default value: N/A
share_type	No	String	Definition: Specifies the bandwidth type. Constraints: • 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. Range: • PER: dedicated bandwidths • WHOLE: shared bandwidths Default value: N/A
billing_info	No	String	Definition: Provides resource billing information. Constraints: N/A Range: N/A Default value: N/A This parameter is unsupported. Please do not use it.

Parameter	Mandatory	Type	Description
id	No	String	Definition: Specifies the ID of the shared bandwidth. An existing shared bandwidth is used. Constraints: The ID must be an existing shared bandwidth ID. There is no need to specify this parameter if the billing mode is yearly/monthly. This parameter will be ignored if it is left blank. Range: N/A Default value: N/A

Table 5-66 CreateLoadbalancerAutoscalingOption

Parameter	Mandatory	Type	Description
enable	Yes	Boolean	Definition: Specifies whether to enable elastic scaling for the load balancer. Constraints: N/A Range: • true: This option will be enabled. • false: This option will be disabled. Default value: N/A
min_l7_flavor_id	No	String	Definition: Specifies the ID of the minimum elastic flavor at Layer 7. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 202

Table 5-67 Response body parameters

Parameter	Type	Description
loadbalancer_ids	Array of strings	Definition: Specifies the IDs of the load balancers to be created in batches. Range: N/A
job_id	String	Definition: Specifies task ID of the batch creation. Range: N/A
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

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 3: 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 3: 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 3: Creating three shared load balancers and binding private IPv4 addresses to them

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudskelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskelb.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.ElClientBuilder().
        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 3: 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.ElClientBuilder().
        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 5-68 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
loadbalancer_id	Yes	String	Definition: Specifies the ID of the load balancer to be upgraded. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-69 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-70 Request body parameters

Parameter	Mandatory	Type	Description
action	Yes	String	Definition: Specifies the action of an upgrade. Constraints: N/A Range: • 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 provisioning_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 provisioning_status of the load balancer is UPGRADED, UPGRADE_FAILED, or ROLLBACK_FAILED. Default value: N/A

Parameter	Mandatory	Type	Description
l4_flavor_id	No	String	Definition: Specifies the ID of a flavor at Layer 4. This parameter is valid only when action is start. Constraints: • 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. Range: N/A Default value: N/A
l7_flavor_id	No	String	Definition: Specifies the ID of a flavor at Layer 7. This parameter is valid only when action is start. Constraints: • 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. Range: N/A Default value: N/A
availability_zone_list	No	Array of strings	Definition: Specifies the list of AZs where the load balancers can be created. 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. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
ipv6_vip_virsubnet_id	No	String	Definition: Specifies the ID of the IPv6 subnet where the load balancer works. You can query parameter id in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets). Constraints: • If you want to use the load balancer to distribute IPv6 requests, this parameter is required. • The subnet defined by ipv6_vip_virsubnet_id must in the VPC where the original shared load balancer works. • IPv6 must be enabled for the subnet defined by ipv6_vip_virsubnet_id. Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
ipv6_vip_address	No	String	Definition: Specifies the private IPv6 address of the load balancer. Constraints: • The IP address must be from the IPv6 subnet where the load balancer resides and should not be used by other services. • 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. Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
elb_virsubnet_ids	No	Array of strings	Definition: Specifies the network 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). Constraints: • This parameter is valid only when action is start. • 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. Range: N/A Default value: N/A

Response Parameters

Status code: 202

Table 5-71 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
job_id	String	Definition: Specifies the upgrade task ID. Range: N/A

Example Requests

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": [ "5eddf5a-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

Successful request.

```
{
  "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

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("5eddf5a-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.getErrMsg());
}
}
```

Python

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

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudskelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskelb.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 = [
            "5eddf5a-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

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.ElClientBuilder().
            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	Successful request.

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 5-72 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Table 5-73 Query Parameters

Parameter	Mandatory	Type	Description
marker	No	String	Definition: Specifies the ID of the last record on the previous page. Constraints: • This parameter must be used together with limit. • If the parameter is not specified, only resources on the first page are queried. • This parameter cannot be left blank or set to an invalid ID. Range: N/A Default value: N/A
limit	No	Integer	Definition: Specifies the number of records returned on each page. Constraints: N/A Range: 0 to 2000 Default value: 2000

Parameter	Mandatory	Type	Description
page_reverse	No	Boolean	Definition: Specifies whether to use reverse query. Constraints: • This parameter must be used together with limit. • If page_reverse is set to true and you want to query the resources on the previous page, set the value of marker to the value of previous_marker. Range: • true: Query resources on the previous page. • false: Query resources on the next page. Default value: false
id	No	Array of strings	Definition: Specifies the load balancer ID. Multiple values can be used for query in the format of: <i>id=xxx&id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
name	No	Array of strings	Definition: Specifies the load balancer name. Multiple values can be used for query in the format of: <i>name=xxx&name=xxx</i> . Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
description	No	Array of strings	Definition: Provides supplementary information about the load balancer. Multiple values can be used for query in the format of: <i>description=xxx&description=xx</i> . Constraints: N/A Range: N/A Default value: N/A
admin_state_up	No	Boolean	Definition: Specifies whether the load balancer is enabled. Constraints: N/A Range: • true: enabled • false: disabled Default value: N/A
include_recycle_bin	No	Boolean	Definition: Specifies whether to query the load balancers in the recycle bin. Constraints: N/A Range: • true: Load balancers in the recycle bin will be returned. • false: Load balancers in the recycle bin will not be returned. Default value: N/A
provisioning_status	No	Array of strings	Definition: Specifies the provisioning status of the load balancer. Multiple values can be used for query in the format of: <i>provisioning_status=xxx&provisioning_status=xxx</i> . Constraints: N/A Range: • ACTIVE: in use • PENDING_DELETE: deleting Default value: N/A

Parameter	Mandatory	Type	Description
operating_status	No	Array of strings	Definition: Specifies the operating status of the load balancer. Multiple values can be used for query in the format of: <i>operating_status=xxx&operating_status=xxx.</i> Constraints: N/A Range: • ONLINE: running • FROZEN: frozen Default value: N/A
guaranteed	No	Boolean	Definition: Specifies whether the load balancer is a dedicated load balancer. Constraints: N/A Range: • false: The load balancer is a shared load balancer. • true: The load balancer is a dedicated load balancer. Default value: N/A
vpc_id	No	Array of strings	Definition: Specifies the ID of the VPC where the load balancer is located. Multiple values can be used for query in the format of: <i>vpc_id=xxx&vpc_id=xxx.</i> Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
<code>vip_port_id</code>	No	Array of strings	Definition: Specifies the ID of the port bound to the private IPv4 address of the load balancer. Multiple values can be used for query in the format of: <i>vip_port_id=xxx&vip_port_id=xx</i> . Constraints: N/A Range: N/A Default value: N/A
<code>vip_address</code>	No	Array of strings	Definition: Specifies the private IPv4 address of the load balancer. Multiple values can be used for query in the format of: <i>vip_address=xxx&vip_address=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
<code>vip_subnet_cidr_id</code>	No	Array of strings	Definition: Specifies the ID of the IPv4 subnet where the load balancer is located. This subnet is also called the frontend subnet. Multiple values can be used for query in the format of: <i>vip_subnet_cidr_id=xxx&vip_subnet_cidr_id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
ipv6_vip_port_id	No	Array of strings	Definition: Specifies the ID of the port bound to the IPv6 address of the load balancer. Multiple values can be used for query in the format of: <i>ipv6_vip_port_id=xxx&ipv6_vip_port_id=xxx.</i> Constraints: N/A Range: N/A Default value: N/A
ipv6_vip_address	No	Array of strings	Definition: Specifies the IPv6 address of the load balancer. Multiple values can be used for query in the format of: <i>ipv6_vip_address=xxx&ipv6_vip_address=xxx.</i> Constraints: N/A Range: N/A Default value: N/A
ipv6_vip_virsubnet_id	No	Array of strings	Definition: Specifies the ID of the IPv6 subnet where the load balancer is located. This subnet is also called the frontend subnet. Multiple values can be used for query in the format of: <i>ipv6_vip_virsubnet_id=xxx&ipv6_vip_virsubnet_id=xxx.</i> Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
eips	No	Array of strings	Definition: Specifies the EIP bound to the load balancer. The following is an example: <pre>"eips": [{ "eip_id": "e9b72a9d-4275-455e- a724-853504e4d9c6", "eip_address": "88.88.14.122", "ip_version": 4 }]</pre> If you want to query the load balancers that have the above EIP bound, you can use the following format: <pre>eips=ip_version %3D4&eips=eip_address %3D88.88.14.122&eips=eip_id %3De9b72a9d-4275-455e- a724-853504e4d9c6</pre> Multiple values can be used for query. • If eip_id is used as the query condition, the format is <i>eips=eip_id=xxx&eips=eip_id=xxx.</i> • If eip_address is used as the query condition, the format is <i>eips=eip_address=xxx&eips=eip_address=xxx.</i> • If ip_version is used as the query condition, the format is <i>eips=ip_version=xxx&eips=ip_version=xxx.</i> Constraints: N/A Range: N/A Default value: N/A Note that this parameter has the same meaning as publicips.

Parameter	Mandatory	Type	Description
publicips	No	Array of strings	Definition: Specifies the EIP bound to the load balancer. The following is an example: <pre>"publicips=": [{ "public_id": "e9b72a9d-4275-455e- a724-853504e4d9c6", "public_address": "88.88.14.122", "ip_version": 4 }]</pre> If you want to query the load balancers that have the above EIP bound, you can use the following format: <pre>publicips=ip_version %3D4&publicips=public_addre ss %3D88.88.14.122&publicips=p ublic_id %3De9b72a9d-4275-455e- a724-853504e4d9c6</pre> Multiple values can be used for query. • If publicip_id is used as the query condition, the format is <i>publicips=publicip_id=xxx&publicips=publicip_id=xxx.</i> • If publicip_address is used as the query condition, the format is <i>publicips=publicip_address=xxx&publicips=publicip_address=xxx.</i> • If ip_version is used as the query condition, the format is <i>publicips=ip_version=xxx&publicips=ip_version=xxx.</i> Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
			Note: This parameter has the same meaning as eips .
availability_zone_list	No	Array of strings	Definition: Specifies the list of AZs where the load balancers are created. Multiple values can be used for query in the format of: <i>availability_zone_list=xxx&availability_zone_list=xxx.</i> Constraints: N/A Range: N/A Default value: N/A
l4_flavor_id	No	Array of strings	Definition: Specifies the ID of a flavor at Layer 4. Multiple values can be used for query in the format of: <i>l4_flavor_id=xxx&l4_flavor_id=xxx.</i> Constraints: N/A Range: N/A Default value: N/A
l4_scale_flavor_id	No	Array of strings	Definition: Specifies the ID of an elastic flavor at Layer 4. Multiple values can be used for query in the format of: <i>l4_scale_flavor_id=xxx&l4_scale_flavor_id=xxx.</i> Constraints: N/A Range: N/A Default value: N/A This parameter is unsupported. Please do not use it.

Parameter	Mandatory	Type	Description
l7_flavor_id	No	Array of strings	Definition: Specifies the ID of a flavor at Layer 7. Multiple values can be used for query in the format of: <i>l7_flavor_id=xxx&l7_flavor_id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
l7_scale_flavor_id	No	Array of strings	Definition: Specifies the ID of an elastic flavor at Layer 7. Multiple values can be used for query in the format of: <i>l7_scale_flavor_id=xxx&l7_scale_flavor_id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A This parameter is unsupported. Please do not use it.
billing_info	No	Array of strings	Definition: Provides resource billing information. Multiple values can be used for query in the format of: <i>billing_info=xxx&billing_info=xx</i> . Constraints: N/A Range: N/A Default value: N/A This parameter is unsupported. Please do not use it.

Parameter	Mandatory	Type	Description
member_device_id	No	Array of strings	Definition: Specifies the ID of the ECS 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 values can be used for query in the format of: <i>member_device_id=xxx&member_device_id=xxx.</i> Constraints: N/A Range: N/A Default value: N/A
member_address	No	Array of strings	Definition: Specifies the private IP address of the ECS 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 values can be used for query in the format of: <i>member_address=xxx&member_address=xxx.</i> Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
enterprise_project_id	No	Array of strings	Definition: Specifies the ID of the enterprise project where the load balancer is used. Multiple values can be used for query in the format of: <i>enterprise_project_id=xxx&enterprise_project_id=xxx.</i> Constraints: • 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. Range: N/A Default value: N/A
ip_version	No	Array of integers	Definition: Specifies the IP address version. Multiple values can be used for query in the format of: <i>ip_version=xxx&ip_version=xxx.</i> Constraints: N/A Range: 4 (IPv4 addresses) or 6 (IPv6 addresses) Default value: N/A

Parameter	Mandatory	Type	Description
deletion_protection_enable	No	Boolean	Definition: Specifies whether to enable deletion protection. Constraints: N/A Range: false (disable this option) or true (enable this option). Default value: N/A
elb_virsubnet_type	No	Array of strings	Definition: Specifies the type of the subnet on the downstream plane. Multiple values can be used for query in the format of: <i>elb_virsubnet_type=ipv4&elb_virsubnet_type=dualstack</i> . Constraints: N/A Range: • ipv4: IPv4 subnets • dualstack: subnets that support IPv4/IPv6 dual stack Default value: N/A
autoscaling	No	Array of strings	Definition: Specifies whether to enable elastic scaling. Example: "autoscaling": { "enable": "true" } Multiple values can be used for query in the format of: <i>autoscaling=enable=true&autoscaling=enable=false</i> . Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
protection_status	No	Array of strings	Definition: Specifies the protection status. Constraints: N/A Range: • nonProtection: The resource is not protected. • consoleProtection: Modification is not allowed on the console. Default value: nonProtection

Parameter	Mandatory	Type	Description
global_eips	No	Array of strings	Definition: Specifies the EIP bound to the load balancer. The following shows an example: <pre>{ "global_eips": [{ "global_eip_id": "240000000-0000-0000-0000-1 000000000001", "global_eip_address": "10.10.10.10", "ip_version": 4 }] }</pre> Multiple values can be used for query in the format of: • If global_eip_id is used as the query condition, the format is <i>global_eips=global_eip_id=xxx&global_eips=global_eip_id=xxx.</i> • If global_eip_address is used as the query condition, the format is <i>global_eips=global_eip_address=xxx&global_eips=global_eip_address=xxx.</i> • If ip_version is used as the query condition, the format is <i>global_eips=ip_version=xxx&global_eips=ip_version=xxx.</i> Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
log_topic_id	No	String	Definition: Specifies the ID of the log topic that is associated with the load balancer. Multiple values can be used for query in the format of: <i>log_topic_id=xxx&log_topic_id=xxx.</i> Constraints: N/A Range: N/A Default value: N/A
log_group_id	No	String	Definition: Specifies the ID of the log group that is associated with the load balancer. Multiple values can be used for query in the format of: <i>log_group_id=xxx&log_group_id=xxx.</i> Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-74 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-75 Response body parameters

Parameter	Type	Description
loadbalancers	Array of LoadBalancer objects	Definition: Lists the load balancers.
page_info	PageInfo object	Definition: Specifies the pagination information.
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

Table 5-76 LoadBalancer

Parameter	Type	Description
id	String	Definition: Specifies the load balancer ID. Range: N/A
description	String	Definition: Provides supplementary information about the load balancer. Range: N/A
provisioning_status	String	Definition: Specifies the provisioning status of the load balancer. Range: • ACTIVE: in use • PENDING_DELETE: deleting
admin_state_up	Boolean	Definition: Specifies whether the load balancer is enabled. Range: • true: enabled • false: disabled
provider	String	Definition: Specifies the provider of the load balancer. The value is fixed to vlb . Range: N/A
pools	Array of PoolRef objects	Definition: Lists the IDs of backend server groups associated with the load balancer.

Parameter	Type	Description
listeners	Array of ListenerRef objects	Definition: Lists the IDs of listeners associated with the load balancer.
operating_status	String	Definition: Specifies the operating status of the load balancer. Range: • ONLINE: The load balancer is online. • FROZEN: The load balancer is frozen.
name	String	Definition: Specifies the load balancer name. Range: N/A
project_id	String	Definition: Specifies the ID of the project where the load balancer is used. Range: N/A
vip_subnet_cidr_id	String	Definition: Specifies the ID of the IPv4 subnet where the load balancer is located. This subnet is also called the frontend subnet. Range: N/A
vip_address	String	Definition: Specifies the private IPv4 address of the load balancer. Range: N/A
vip_port_id	String	Definition: Specifies the ID of the port bound to the private IPv4 address of the load balancer. Range: N/A
tags	Array of Tag objects	Definition: Specifies the tags added to the load balancer.
created_at	String	Definition: Specifies the time when the load balancer was created. Range: The value must be in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> .

Parameter	Type	Description
updated_at	String	Definition: Specifies the time when the load balancer was updated. Range: The value must be in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> .
guaranteed	Boolean	Definition: Specifies whether the load balancer is a dedicated load balancer. Range: • false: The load balancer is a shared load balancer. • true: The load balancer is a dedicated load balancer.
vpc_id	String	Definition: Specifies the ID of the VPC where the load balancer is located. Range: N/A
eips	Array of EipInfo objects	Definition: Specifies the EIP bound to the load balancer. NOTE This parameter has the same meaning as publicips .
ipv6_vip_address	String	Definition: Specifies the IPv6 address of the load balancer. Range: N/A
ipv6_vip_virsubnet_id	String	Definition: Specifies the ID of the IPv6 subnet where the load balancer is located. This subnet is also called the frontend subnet. Range: N/A
ipv6_vip_port_id	String	Definition: Specifies the ID of the port bound to the IPv6 address of the load balancer. Range: N/A
availability_zone_list	Array of strings	Definition: Specifies the list of AZs where the load balancers are created. Range: N/A

Parameter	Type	Description
enterprise_project_id	String	Definition: Specifies the ID of the enterprise project. Range: • 0: The resource belongs to the default enterprise project. • A string in UUID format indicates a non-default enterprise project.
billing_info	String	Definition: Provides resource billing information. Range: • If the value is left blank, the resource is billed on a pay-per-use basis. This parameter is unsupported. Please do not use it.
l4_flavor_id	String	Definition: Specifies the ID of a flavor at Layer 4. If the current load balancer is an elastic flavor instance, this parameter defines the maximum elastic flavor at Layer 4. Range: N/A
l4_scale_flavor_id	String	Definition: Specifies the ID of an elastic flavor at Layer 4. Range: N/A NOTE This parameter has been discarded. Do not use it.
l7_flavor_id	String	Definition: Specifies the ID of a flavor at Layer 7. If the current load balancer is an elastic flavor instance, this parameter defines the maximum elastic flavor at Layer 7. Range: N/A
l7_scale_flavor_id	String	Definition: Specifies the ID of an elastic flavor at Layer 7. Range: N/A NOTE This parameter has been discarded. Do not use it.

Parameter	Type	Description
gw_flavor_id	String	Definition: Specifies the flavor ID of the gateway load balancer. Range: N/A This parameter is unsupported. Please do not use it.
loadbalancer_type	String	Definition: Specifies the load balancer type. Range: • gateway: gateway load balancers • null: other types of load balancers This parameter is unsupported. Please do not use it.
publicips	Array of PublicIpInfo objects	Definition: Specifies the EIP bound to the load balancer. NOTE This parameter has the same meaning as eips .
global_eips	Array of GlobalEipInfo objects	Definition: Specifies the global EIP bound to the load balancer.
elb_virsubnet_ids	Array of strings	Definition: Specifies the network IDs of subnets on the downstream plane. Range: N/A
elb_virsubnet_type	String	Definition: Specifies the type of the subnet on the downstream plane. Range: • ipv4: IPv4 subnets • dualstack: subnets that support IPv4/IPv6 dual stack

Parameter	Type	Description
ip_target_enable	Boolean	Definition: Specifies whether to add backend servers that are not in the load balancer's VPC. 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. Range: • true: This option will be enabled. • false: This option will be disabled.
frozen_scene	String	Definition: Specifies the scenario where the load balancer is frozen. If there are multiple scenarios, separate them with commas (,). Range: • 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. • AREAR: The load balancer is frozen due to arrears.
deletion_protection_enable	Boolean	Definition: Specifies whether to enable deletion protection. This parameter is returned only when the deletion protection is enabled in the current region. Range: • false: This option will be disabled. • true: This option will be enabled.

Parameter	Type	Description
autoscaling	AutoscalingRef object	Definition: Specifies information about elastic scaling. If elastic scaling is enabled, the load balancer flavors can be automatically adjusted based on incoming traffic. NOTE 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 flavors will be created and you will be billed for the minimum flavors.
public_border_group	String	Definition: Specifies the public border group. Range: • center: public border group of the central site • Edge site name: public border group of an edge site
charge_mode	String	Definition: Specifies the charge mode of the load balancer. Range: • flavor: billed by the fixed flavor you select. • lcu: billed by how many LCUs you have used. • Null: If it is a shared load balancer, it is free. If it is a dedicated load balancer, it will be billed by the fixed flavor you select. This parameter is unsupported. Please do not use it.
service_lb_mode	String	Definition: Specifies load balancer mode. Range: • lb: Cross-tenant access is not supported. • ep: Cross-tenant access is supported. This parameter is unsupported. Please do not use it.

Parameter	Type	Description
instance_type	String	Definition: Specifies the internal service to which the load balancer belongs. Range: N/A This parameter is unsupported. Please do not use it.
instance_id	String	Definition: Specifies the ID of the instance with which the load balancer is associated. Range: N/A This parameter is unsupported. Please do not use it.
proxy_protocol_extensions	Array of ProxyProtocolExtension objects	Definition: Specifies the proxy protocol extension. This parameter is unsupported. Please do not use it.
waf_failure_action	String	Definition: Specifies traffic distributing policies when the WAF is faulty. Range: discard indicates traffic will not be distributed. forward indicates traffic will be distributed to the default backend servers.
protection_status	String	Definition: Specifies the protection status. Range: • nonProtection: The resource is not protected. • consoleProtection: Modification is not allowed on the console.
protection_reason	String	Definition: Specifies why modification protection is enabled. Range: The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).
log_group_id	String	Definition: Specifies the ID of the log group that is associated with the load balancer. Range: N/A
log_topic_id	String	Definition: Specifies the ID of the log topic that is associated with the load balancer. Range: N/A

Parameter	Type	Description
custom_qos_limit	CustomQosLimit object	Definition: Specifies the rate limit information of the ELB flavors. Range: N/A This parameter is unsupported. Please do not use it.

Table 5-77 PoolRef

Parameter	Type	Description
id	String	Definition: Specifies the backend server group ID. Range: N/A

Table 5-78 ListenerRef

Parameter	Type	Description
id	String	Definition: Specifies the listener ID. Range: N/A

Table 5-79 Tag

Parameter	Type	Description
key	String	Definition: Specifies the tag key. Range: N/A
value	String	Definition: Specifies the tag value. Range: N/A

Table 5-80 EipInfo

Parameter	Type	Description
eip_id	String	Definition: Specifies the EIP ID. Range: N/A
eip_address	String	Definition: Specifies the EIP. Range: N/A

Parameter	Type	Description
ip_version	Integer	Definition: Specifies the IP address version. Range: • 4: IPv4 addresses • 6: IPv6 addresses

Table 5-81 PublicIpInfo

Parameter	Type	Description
publicip_id	String	Definition: Specifies the EIP ID. Range: N/A
publicip_address	String	Definition: Specifies the EIP. Range: N/A
ip_version	Integer	Definition: Specifies the IP address version. Range: • 4: IPv4 address • 6: IPv6 address

Table 5-82 GlobalEipInfo

Parameter	Type	Description
global_eip_id	String	Definition: Specifies the ID of the global EIP. Range: N/A
global_eip_addresses	String	Definition: Specifies the global EIP. Range: N/A
ip_version	Integer	Definition: Specifies the IP address version. Range: • 4: IPv4 addresses • 6: IPv6 addresses

Table 5-83 AutoscalingRef

Parameter	Type	Description
enable	Boolean	Definition: Specifies whether to enable elastic scaling for the load balancer. Range: • true: This option will be enabled. • false: This option will be disabled.
min_l7_flavor_id	String	Definition: Specifies the ID of the minimum elastic flavor at Layer 7. Range: N/A

Table 5-84 ProxyProtocolExtension

Parameter	Type	Description
vip_address	String	Definition: Specifies the IPv4 address. Constraints: N/A Range: N/A Default value: N/A
ipv6_vip_address	String	Definition: Specifies the IPv6 address. Constraints: N/A Range: N/A Default value: N/A
extension	Extension object	Definition: Specifies the proxy protocol extension. Constraints: N/A

Table 5-85 Extension

Parameter	Type	Description
ep_id	String	Definition: Specifies the VPC endpoint ID. Constraints: N/A Range: N/A Default value: N/A

Parameter	Type	Description
ep_service_id	String	Definition: Specifies the VPC endpoint service ID. Constraints: N/A Range: N/A Default value: N/A

Table 5-86 CustomQosLimit

Parameter	Type	Description
l4	L4Limit object	Definition: Specifies the rate limit information of the ELB flavors at Layer 4.
l7	L7Limit object	Definition: Specifies the rate limit information of the ELB flavors at Layer 7.

Table 5-87 L4Limit

Parameter	Type	Description
connection	Integer	Definition: Specifies the maximum number of concurrent connections at Layer 4. Range: N/A
cps	Integer	Definition: Specifies the maximum number of new connections at Layer 4. Range: N/A

Table 5-88 L7Limit

Parameter	Type	Description
connection	Integer	Definition: Specifies the maximum number of concurrent connections at Layer 7. Range: N/A
cps	Integer	Definition: Specifies the maximum number of new connections at Layer 7. Range: N/A

Table 5-89 PageInfo

Parameter	Type	Description
previous_marker	String	Definition: Specifies the ID of the first record in the pagination query result. If page_reverse is set to true , this parameter is used together to query resources on the previous page. Range: N/A
next_marker	String	Definition: Specifies the ID of the last record in the pagination query result. It is usually used to query resources on the next page. Range: N/A
current_count	Integer	Definition: Specifies the number of records returned on the current page. Range: N/A

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

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudskelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskelb.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 5-90 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
loadbalancer_id	Yes	String	Definition: Specifies the load balancer ID. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-91 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-92 Request body parameters

Parameter	Mandatory	Type	Description
count	No	Integer	Definition: Specifies the maximum number of replicas at a time. Constraints: N/A Range: 1 to 10 Default value: 1

Parameter	Mandatory	Type	Description
target_loadbalancer_param	Yes	TargetLoadbalancerParam object	Definition: Specifies the parameters of the new load balancer. Constraints: N/A

Table 5-93 TargetLoadbalancerParam

Parameter	Mandatory	Type	Description
name	No	String	Definition: Specifies the name of the new load balancer. Constraints: N/A Range: N/A Default value: If this parameter is not specified, the new load balancer name will be the original load balancer name plus suffix copy-x. x indicates the serial number.
availability_zone_list	No	Array of strings	Definition: Specifies the AZ where new load balancer works. Constraints: This parameter is available only for copying a dedicated load balancer. Range: N/A Default value: If this parameter is not specified, the AZs defined in availability_zone_list of the original load balancer will be used.

Parameter	Mandatory	Type	Description
vip_subnet_cidr_id	No	String	Definition: Specifies the ID of the IPv4 subnet where the new load balancer works. Constraints: The subnets where the original and new load balancers work must be in the same VPC. Range: N/A Default value: If this parameter is not specified, the IPv4 subnet defined by vip_subnet_cidr_id of the original load balancer is used.
vip_address	No	String	Definition: Specifies the private IPv4 address of the new load balancer. Constraints: This parameter is available only when you copy a dedicated or shared load balancer as a dedicated load balancer. Range: N/A Default value: If this parameter is not specified, a private IPv4 address in the subnet defined by vip_subnet_cidr_id will be randomly assigned to the new load balancer.
ipv6_vip_virusubnet_id	No	String	Definition: Specifies the ID of the IPv6 subnet where the new load balancer works. Constraints: • This parameter is available only for copying a dedicated load balancer. • The subnets where the original and new load balancers work must be in the same VPC. Range: N/A Default value: If this parameter is not specified, the IPv6 subnet defined by ipv6_vip_virusubnet_id of the original load balancer is used.

Parameter	Mandatory	Type	Description
ipv6_vip_address	No	String	Definition: Specifies the private IPv6 address of the new load balancer. Constraints: This parameter is available only for copying a dedicated load balancer. Range: N/A Default value: If this parameter is not specified, a private IPv6 address in the subnet defined by ipv6_vip_virsubnet_id will be randomly assigned to the new load balancer.
elb_virsubnet_ids	No	Array of strings	Definition: Specifies the ID of the backend subnet of the new load balancer. Constraints: • This parameter is available only when you copy a dedicated or shared load balancer as a dedicated load balancer. • The subnets where the original and new load balancers work must be in the same VPC. Range: N/A Default value: If this parameter is not specified, the backend subnet of the original load balancer is used.
l4_flavor_id	No	String	Definition: Specifies the Layer 4 flavor of the new load balancer. Constraints: This parameter is available only when you copy a dedicated or shared load balancer as a dedicated load balancer. Range: N/A Default value: If this parameter is not specified, the Layer 4 flavor of the original load balancer is used.

Parameter	Mandatory	Type	Description
l7_flavor_id	No	String	Definition: Specifies the Layer 7 flavor of the new load balancer. Constraints: This parameter is available only when you copy a dedicated or shared load balancer as a dedicated load balancer. Range: N/A Default value: If this parameter is not specified, the Layer 7 flavor of the original load balancer is used.
enterprise_project_id	No	String	Definition: Specifies the ID of the enterprise project. Constraints: N/A Range: N/A Default value: If this parameter is not specified, the enterprise project of the original load balancer is used.

Parameter	Mandatory	Type	Description
reuse_pool	No	Boolean	Definition: Specifies whether to reuse the backend server group of the original load balancer. Constraints: • 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 the ID of another enterprise project. • This parameter can be set to true only when you copy a dedicated or shared load balancer as a dedicated load balancer. Range: • false: A new backend server group will be created and associated with the new load balancer. • true: The backend server group of the original load balancer will be used. Default value: false

Parameter	Mandatory	Type	Description
guaranteed	No	Boolean	Definition: Specifies the type of the new load balancer. Constraints: N/A Range: • false: A new shared load balancer will be created. The original load balancer must be a shared load balancer. • true: A dedicated load balancer will be created. The original load balancer can be a shared or dedicated load balancer. Default value: • true if the original load balancer is a dedicated load balancer. • false if the original load balancer is a shared load balancer.

Response Parameters

Status code: 200

Table 5-94 Response body parameters

Parameter	Type	Description
loadbalancer_list	Array of loadbalancer_list objects	Definition: Specifies the information about the new load balancer. Range: N/A
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
job_id	String	Definition: Specifies the copy task ID. Range: N/A

Table 5-95 loadbalancer_list

Parameter	Type	Description
id	String	Definition: Specifies the ID of the new load balancer. Range: N/A

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.getStatusCode());
    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 huaweicloudskelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskelb.v3 import *

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

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

client = 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 5-96 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
loadbalancer_id	Yes	String	Definition: Specifies the load balancer ID. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-97 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-98 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

Parameter	Type	Description
loadbalancer	LoadBalancer object	Definition: Provides details about the load balancer.

Table 5-99 LoadBalancer

Parameter	Type	Description
id	String	Definition: Specifies the load balancer ID. Range: N/A
description	String	Definition: Provides supplementary information about the load balancer. Range: N/A
provisioning_status	String	Definition: Specifies the provisioning status of the load balancer. Range: • ACTIVE: in use • PENDING_DELETE: deleting
admin_state_up	Boolean	Definition: Specifies whether the load balancer is enabled. Range: • true: enabled • false: disabled
provider	String	Definition: Specifies the provider of the load balancer. The value is fixed to vlb . Range: N/A
pools	Array of PoolRef objects	Definition: Lists the IDs of backend server groups associated with the load balancer.
listeners	Array of ListenerRef objects	Definition: Lists the IDs of listeners associated with the load balancer.
operating_status	String	Definition: Specifies the operating status of the load balancer. Range: • ONLINE: The load balancer is online. • FROZEN: The load balancer is frozen.

Parameter	Type	Description
name	String	Definition: Specifies the load balancer name. Range: N/A
project_id	String	Definition: Specifies the ID of the project where the load balancer is used. Range: N/A
vip_subnet_cidr_id	String	Definition: Specifies the ID of the IPv4 subnet where the load balancer is located. This subnet is also called the frontend subnet. Range: N/A
vip_address	String	Definition: Specifies the private IPv4 address of the load balancer. Range: N/A
vip_port_id	String	Definition: Specifies the ID of the port bound to the private IPv4 address of the load balancer. Range: N/A
tags	Array of Tag objects	Definition: Specifies the tags added to the load balancer.
created_at	String	Definition: Specifies the time when the load balancer was created. Range: The value must be in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> .
updated_at	String	Definition: Specifies the time when the load balancer was updated. Range: The value must be in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> .
guaranteed	Boolean	Definition: Specifies whether the load balancer is a dedicated load balancer. Range: • false: The load balancer is a shared load balancer. • true: The load balancer is a dedicated load balancer.

Parameter	Type	Description
vpc_id	String	Definition: Specifies the ID of the VPC where the load balancer is located. Range: N/A
eips	Array of EipInfo objects	Definition: Specifies the EIP bound to the load balancer. NOTE This parameter has the same meaning as publicips .
ipv6_vip_address	String	Definition: Specifies the IPv6 address of the load balancer. Range: N/A
ipv6_vip_virsubnet_id	String	Definition: Specifies the ID of the IPv6 subnet where the load balancer is located. This subnet is also called the frontend subnet. Range: N/A
ipv6_vip_port_id	String	Definition: Specifies the ID of the port bound to the IPv6 address of the load balancer. Range: N/A
availability_zone_list	Array of strings	Definition: Specifies the list of AZs where the load balancers are created. Range: N/A
enterprise_project_id	String	Definition: Specifies the ID of the enterprise project. Range: • 0: The resource belongs to the default enterprise project. • A string in UUID format indicates a non-default enterprise project.
billing_info	String	Definition: Provides resource billing information. Range: • If the value is left blank, the resource is billed on a pay-per-use basis. This parameter is unsupported. Please do not use it.

Parameter	Type	Description
l4_flavor_id	String	Definition: Specifies the ID of a flavor at Layer 4. If the current load balancer is an elastic flavor instance, this parameter defines the maximum elastic flavor at Layer 4. Range: N/A
l4_scale_flavor_id	String	Definition: Specifies the ID of an elastic flavor at Layer 4. Range: N/A NOTE This parameter has been discarded. Do not use it.
l7_flavor_id	String	Definition: Specifies the ID of a flavor at Layer 7. If the current load balancer is an elastic flavor instance, this parameter defines the maximum elastic flavor at Layer 7. Range: N/A
l7_scale_flavor_id	String	Definition: Specifies the ID of an elastic flavor at Layer 7. Range: N/A NOTE This parameter has been discarded. Do not use it.
gw_flavor_id	String	Definition: Specifies the flavor ID of the gateway load balancer. Range: N/A This parameter is unsupported. Please do not use it.
loadbalancer_type	String	Definition: Specifies the load balancer type. Range: • gateway: gateway load balancers • null: other types of load balancers This parameter is unsupported. Please do not use it.
publicips	Array of PublicIpInfo objects	Definition: Specifies the EIP bound to the load balancer. NOTE This parameter has the same meaning as eips .

Parameter	Type	Description
global_eips	Array of GlobalEipInfo objects	Definition: Specifies the global EIP bound to the load balancer.
elb_virsubnet_ids	Array of strings	Definition: Specifies the network IDs of subnets on the downstream plane. Range: N/A
elb_virsubnet_type	String	Definition: Specifies the type of the subnet on the downstream plane. Range: • ipv4: IPv4 subnets • dualstack: subnets that support IPv4/IPv6 dual stack
ip_target_enable	Boolean	Definition: Specifies whether to add backend servers that are not in the load balancer's VPC. 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. Range: • true: This option will be enabled. • false: This option will be disabled.
frozen_scene	String	Definition: Specifies the scenario where the load balancer is frozen. If there are multiple scenarios, separate them with commas (,). Range: • 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. • AREAR: The load balancer is frozen due to arrears.

Parameter	Type	Description
deletion_protection_enable	Boolean	Definition: Specifies whether to enable deletion protection. This parameter is returned only when the deletion protection is enabled in the current region. Range: • false: This option will be disabled. • true: This option will be enabled.
autoscaling	AutoscalingRef object	Definition: Specifies information about elastic scaling. If elastic scaling is enabled, the load balancer flavors can be automatically adjusted based on incoming traffic. NOTE 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 flavors will be created and you will be billed for the minimum flavors.
public_border_group	String	Definition: Specifies the public border group. Range: • center: public border group of the central site • Edge site name: public border group of an edge site
charge_mode	String	Definition: Specifies the charge mode of the load balancer. Range: • flavor: billed by the fixed flavor you select. • lcu: billed by how many LCUs you have used. • Null: If it is a shared load balancer, it is free. If it is a dedicated load balancer, it will be billed by the fixed flavor you select. This parameter is unsupported. Please do not use it.

Parameter	Type	Description
service_lb_mode	String	Definition: Specifies load balancer mode. Range: • lb: Cross-tenant access is not supported. • ep: Cross-tenant access is supported. This parameter is unsupported. Please do not use it.
instance_type	String	Definition: Specifies the internal service to which the load balancer belongs. Range: N/A This parameter is unsupported. Please do not use it.
instance_id	String	Definition: Specifies the ID of the instance with which the load balancer is associated. Range: N/A This parameter is unsupported. Please do not use it.
proxy_protocol_extensions	Array of ProxyProtocolExtension objects	Definition: Specifies the proxy protocol extension. This parameter is unsupported. Please do not use it.
waf_failure_action	String	Definition: Specifies traffic distributing policies when the WAF is faulty. Range: discard indicates traffic will not be distributed. forward indicates traffic will be distributed to the default backend servers.
protection_status	String	Definition: Specifies the protection status. Range: • nonProtection: The resource is not protected. • consoleProtection: Modification is not allowed on the console.

Parameter	Type	Description
protection_reason	String	Definition: Specifies why modification protection is enabled. Range: The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).
log_group_id	String	Definition: Specifies the ID of the log group that is associated with the load balancer. Range: N/A
log_topic_id	String	Definition: Specifies the ID of the log topic that is associated with the load balancer. Range: N/A
custom_qos_limit	CustomQosLimit object	Definition: Specifies the rate limit information of the ELB flavors. Range: N/A This parameter is unsupported. Please do not use it.

Table 5-100 PoolRef

Parameter	Type	Description
id	String	Definition: Specifies the backend server group ID. Range: N/A

Table 5-101 ListenerRef

Parameter	Type	Description
id	String	Definition: Specifies the listener ID. Range: N/A

Table 5-102 Tag

Parameter	Type	Description
key	String	Definition: Specifies the tag key. Range: N/A

Parameter	Type	Description
value	String	Definition: Specifies the tag value. Range: N/A

Table 5-103 EipInfo

Parameter	Type	Description
eip_id	String	Definition: Specifies the EIP ID. Range: N/A
eip_address	String	Definition: Specifies the EIP. Range: N/A
ip_version	Integer	Definition: Specifies the IP address version. Range: • 4: IPv4 addresses • 6: IPv6 addresses

Table 5-104 PublicIpInfo

Parameter	Type	Description
publicip_id	String	Definition: Specifies the EIP ID. Range: N/A
publicip_address	String	Definition: Specifies the EIP. Range: N/A
ip_version	Integer	Definition: Specifies the IP address version. Range: • 4: IPv4 address • 6: IPv6 address

Table 5-105 GlobalEipInfo

Parameter	Type	Description
global_eip_id	String	Definition: Specifies the ID of the global EIP. Range: N/A

Parameter	Type	Description
global_eip_addresses	String	Definition: Specifies the global EIP. Range: N/A
ip_version	Integer	Definition: Specifies the IP address version. Range: • 4: IPv4 addresses • 6: IPv6 addresses

Table 5-106 AutoscalingRef

Parameter	Type	Description
enable	Boolean	Definition: Specifies whether to enable elastic scaling for the load balancer. Range: • true: This option will be enabled. • false: This option will be disabled.
min_l7_flavor_id	String	Definition: Specifies the ID of the minimum elastic flavor at Layer 7. Range: N/A

Table 5-107 ProxyProtocolExtension

Parameter	Type	Description
vip_address	String	Definition: Specifies the IPv4 address. Constraints: N/A Range: N/A Default value: N/A
ipv6_vip_address	String	Definition: Specifies the IPv6 address. Constraints: N/A Range: N/A Default value: N/A
extension	Extension object	Definition: Specifies the proxy protocol extension. Constraints: N/A

Table 5-108 Extension

Parameter	Type	Description
ep_id	String	Definition: Specifies the VPC endpoint ID. Constraints: N/A Range: N/A Default value: N/A
ep_service_id	String	Definition: Specifies the VPC endpoint service ID. Constraints: N/A Range: N/A Default value: N/A

Table 5-109 CustomQosLimit

Parameter	Type	Description
l4	L4Limit object	Definition: Specifies the rate limit information of the ELB flavors at Layer 4.
l7	L7Limit object	Definition: Specifies the rate limit information of the ELB flavors at Layer 7.

Table 5-110 L4Limit

Parameter	Type	Description
connection	Integer	Definition: Specifies the maximum number of concurrent connections at Layer 4. Range: N/A
cps	Integer	Definition: Specifies the maximum number of new connections at Layer 4. Range: N/A

Table 5-111 L7Limit

Parameter	Type	Description
connection	Integer	Definition: Specifies the maximum number of concurrent connections at Layer 7. Range: N/A
cps	Integer	Definition: Specifies the maximum number of new connections at Layer 7. Range: N/A

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

```
}  
}
```

Python

```
# coding: utf-8  
  
import os  
from huaweicloudsdkcore.auth.credentials import BasicCredentials  
from huaweicloudskelb.v3.region.elb_region import ElbRegion  
from huaweicloudsdkcore.exceptions import exceptions  
from huaweicloudskelb.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 5-112 Path Parameters

Parameter	Mandatory	Type	Description
loadbalancer_id	Yes	String	Definition: Specifies the load balancer ID. Constraints: N/A Range: N/A Default value: N/A
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-113 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-114 Request body parameters

Parameter	Mandatory	Type	Description
loadbalancer	Yes	UpdateLoadBalancerOptions object	Definition: Specifies the parameters for updating a load balancer. Constraints: N/A

Table 5-115 UpdateLoadBalancerOption

Parameter	Mandatory	Type	Description
name	No	String	Definition: Specifies the load balancer name. Constraints: N/A Range: The value can contain a maximum of 255 Unicode characters, including letters and more. It can be left blank. Default value: N/A
admin_state_up	No	Boolean	Definition: Specifies whether the load balancer is enabled. Range: • true: enabled • false: disabled Constraints: N/A Range: N/A Default value: N/A
description	No	String	Definition: Provides supplementary information about the load balancer. Constraints: N/A Range: The value can contain a maximum of 255 Unicode characters, including letters and more. It can be left blank. Default value: N/A

Parameter	Mandatory	Type	Description
ipv6_vip_virsubnet_id	No	String	Definition: Specifies the ID of the IPv6 subnet where the load balancer is located. This subnet is also called the frontend subnet. You can query parameter neutron_network_id in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets). Updating ipv6_vip_virsubnet_id changes the IPv6 subnet where the load balancer is located, and new IPv6 addresses will be assigned to the load balancer. However, the IPv4 subnet will not change. Constraints: • The subnet specified by ipv6_vip_virsubnet_id must be in the VPC specified by vpc_id, and this subnet must support IPv6. • This parameter can be updated only when guaranteed is set to true. Range: The ID must be in UUID format and can contain up to 36 characters. Default value: N/A NOTE If this parameter is set to null, the IPv6 addresses will be unbound from the load balancer. Do not specify this parameter if no IPv6 subnet needs to be changed.

Parameter	Mandatory	Type	Description
<code>vip_subnet_cidr_id</code>	No	String	Definition: Specifies the ID of the IPv4 subnet where the load balancer is located. This subnet is also called the frontend subnet. You can query parameter neutron_subnet_id in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets). Updating vip_subnet_cidr_id changes the IPv4 subnet where the load balancer is located, and new IPv4 addresses will be assigned to the load balancer. However, the IPv6 subnet will not change. Constraints: • If vip_address is also specified, the IP address specified by vip_address must be in the subnet specified by vip_subnet_cidr_id. • The subnet specified by vip_subnet_cidr_id must in the VPC specified by vpc_id. • This parameter can be updated only when guaranteed is set to true. Range: The ID must be in UUID format and can contain up to 36 characters. Default value: N/A NOTE If this parameter is set to null, the IPv4 addresses will be unbound from the load balancer. Do not specify this parameter if no IPv4 subnet needs to be changed.

Parameter	Mandatory	Type	Description
vip_address	No	String	Definition: Specifies the private IPv4 address of the load balancer. Constraints: The IP address must be from the IPv4 subnet where the load balancer resides and should not be occupied by other services. Range: The IP address must be in [0-255].[0-255].[0-255].[0-255] format, for example, 192.168.1.1. Default value: N/A Note: This parameter can be updated only when guaranteed is set to true.

Parameter	Mandatory	Type	Description
l4_flavor_id	No	String	Definition: Specifies the ID of a flavor at Layer 4. You can query parameter id in the response by calling the API (GET https://{ELB_Endpoint}/v3/{project_id}/elb/flavors?type=L4). Constraints: • 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 flavor type is L4, the load balancer uses the fixed flavors and will be billed by the flavor you select. • If the flavor type is L4_elastic_max, the load balancer uses the elastic flavors and will be billed by how many LCUs you use. Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
l7_flavor_id	No	String	Definition: Specifies the ID of a flavor at Layer 7. You can query parameter id in the response by calling the API (GET https://{ELB_Endpoint}/v3/{project_id}/elb/flavors?type=L7). Constraints: • 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 flavor type is L7, the load balancer uses the fixed flavors and will be billed by the flavor you select. • If the flavor type is L7_elastic_max, the load balancer uses the elastic flavors and will be billed by how many LCUs you use. Range: N/A Default value: N/A
ipv6_bandwidth	No	BandwidthRef object	Definition: Specifies the ID of the bandwidth. Constraints: • This parameter is available only when you create or update a load balancer with a public address. • If you bind a new EIP to the load balancer and specify a shared bandwidth, this EIP will be added to the shared bandwidth.

Parameter	Mandatory	Type	Description
ip_target_enable	No	Boolean	Definition: Specifies whether to add backend servers that are not in the load balancer's VPC. 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. Constraints: • This function cannot be disabled once it is enabled. • If you want to enable IP as a Backend for a load balancer in a shared VPC, ensure that a VPC peering connection has been created to connect the VPCs. Otherwise, the communication will fail. • This function is supported only by dedicated load balancers. Range: • true: This option will be enabled. • false: This option will be disabled. Default value: N/A

Parameter	Mandatory	Type	Description
elb_virsubnet_ids	No	Array of strings	Definition: Specifies the network 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). Constraints: • If the IDs of the subnets bound to 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 bound to 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. • 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. • All subnets specified by elb_virsubnet_ids must in the VPC where the load balancer works. • Edge subnets are not supported. Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
deletion_protection_enable	No	Boolean	Definition: Specifies whether to enable deletion protection. Constraints: Disable deletion protection or removal protection for your resources before deregistering your account. Range: false (disable this option) or true (enable this option). Default value: N/A
prepaid_options	No	PrepaidUpdateOption object	Definition: Specifies the prepaid billing configuration for updating a load balancer. This parameter is unsupported. Please do not use it.
autoscaling	No	UpdateLoadBalancerAutoScalingOption object	Definition: Specifies information about elastic scaling. If elastic scaling is enabled, the load balancer flavors can be automatically adjusted based on incoming traffic. Constraints: • This parameter is only available for whitelisted users. • 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. NOTE 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 flavors will be created and you will be billed for the minimum flavors.

Parameter	Mandatory	Type	Description
charge_mode	No	String	Definition: Specifies the charge mode of the load balancer. Constraints: N/A Range: • flavor: billed by the fixed flavor you select. Default value: N/A
waf_failure_action	No	String	Definition: Specifies traffic distributing policies when the WAF is faulty. Constraints: This parameter takes effect only when WAF is enabled for the load balancer. Range: discard indicates traffic will not be distributed. forward indicates traffic will be distributed to the default backend servers. Default value: forward
protection_status	No	String	Definition: Specifies the protection status. Constraints: N/A Range: • nonProtection: The resource is not protected. • consoleProtection: Modification is not allowed on the console. Default value: N/A
protection_reason	No	String	Definition: Specifies why modification protection is enabled. Constraints: This parameter is valid only when protection_status is set to consoleProtection . Range: The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>). Default value: N/A

Parameter	Mandatory	Type	Description
ipv6_vip_address	No	String	Definition: Specifies the IPv6 address of the load balancer. Constraints: N/A Range: N/A Default value: N/A

Table 5-116 BandwidthRef

Parameter	Mandatory	Type	Description
id	Yes	String	Definition: Specifies the ID of the shared bandwidth. Constraints: N/A Range: N/A Default value: N/A

Table 5-117 PrepaidUpdateOption

Parameter	Mandatory	Type	Description
auto_pay	No	Boolean	Definition: Specifies whether the payment will be automatically deducted from your account balance when an order is submitted. Constraints: If you use the automatic payment mode, only your account balance can be used. If you want to use a voucher, do not use the automatic payment mode, and select the voucher for the payment in the Billing Center. Range: • true: The order will be automatically paid. • false: The order will not be automatically paid. Default value: N/A

Parameter	Mandatory	Type	Description
change_mode	No	String	Definition: Specifies the flavor change type. Constraints: N/A Range: • immediate: The flavor change is applied immediately. • delay: The flavor change is applied after the current subscription period ends. Default value: N/A
period_num	No	Integer	Definition: Specifies the number of subscription periods. The value varies with the operation policy. Constraints: This parameter takes effect only when change_mode is set to delay . Range: • 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. Default value: N/A
period_type	No	String	Definition: Specifies the subscription period type. Constraints: This parameter takes effect only when change_mode is set to delay . Range: • month: monthly subscription • year: yearly subscription Default value: N/A

Table 5-118 UpdateLoadbalancerAutoscalingOption

Parameter	Mandatory	Type	Description
enable	Yes	Boolean	Definition: Specifies whether to enable elastic scaling for the load balancer. Constraints: N/A Range: • true: This option will be enabled. • false: This option will be disabled. Default value: N/A
min_l7_flavor_id	No	String	Definition: Specifies the ID of the minimum elastic flavor at Layer 7. Constraints: This parameter cannot be left blank if there are Layer 7 listeners. Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-119 Response body parameters

Parameter	Type	Description
loadbalancer	LoadBalancer object	Definition: Specifies the load balancer.
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

Table 5-120 LoadBalancer

Parameter	Type	Description
id	String	Definition: Specifies the load balancer ID. Range: N/A
description	String	Definition: Provides supplementary information about the load balancer. Range: N/A
provisioning_status	String	Definition: Specifies the provisioning status of the load balancer. Range: • ACTIVE: in use • PENDING_DELETE: deleting
admin_state_up	Boolean	Definition: Specifies whether the load balancer is enabled. Range: • true: enabled • false: disabled
provider	String	Definition: Specifies the provider of the load balancer. The value is fixed to vlb . Range: N/A
pools	Array of PoolRef objects	Definition: Lists the IDs of backend server groups associated with the load balancer.
listeners	Array of ListenerRef objects	Definition: Lists the IDs of listeners associated with the load balancer.
operating_status	String	Definition: Specifies the operating status of the load balancer. Range: • ONLINE: The load balancer is online. • FROZEN: The load balancer is frozen.
name	String	Definition: Specifies the load balancer name. Range: N/A

Parameter	Type	Description
project_id	String	Definition: Specifies the ID of the project where the load balancer is used. Range: N/A
vip_subnet_cidr_id	String	Definition: Specifies the ID of the IPv4 subnet where the load balancer is located. This subnet is also called the frontend subnet. Range: N/A
vip_address	String	Definition: Specifies the private IPv4 address of the load balancer. Range: N/A
vip_port_id	String	Definition: Specifies the ID of the port bound to the private IPv4 address of the load balancer. Range: N/A
tags	Array of Tag objects	Definition: Specifies the tags added to the load balancer.
created_at	String	Definition: Specifies the time when the load balancer was created. Range: The value must be in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> .
updated_at	String	Definition: Specifies the time when the load balancer was updated. Range: The value must be in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> .
guaranteed	Boolean	Definition: Specifies whether the load balancer is a dedicated load balancer. Range: • false: The load balancer is a shared load balancer. • true: The load balancer is a dedicated load balancer.
vpc_id	String	Definition: Specifies the ID of the VPC where the load balancer is located. Range: N/A

Parameter	Type	Description
eips	Array of EipInfo objects	Definition: Specifies the EIP bound to the load balancer. NOTE This parameter has the same meaning as publicips .
ipv6_vip_address	String	Definition: Specifies the IPv6 address of the load balancer. Range: N/A
ipv6_vip_virsubnet_id	String	Definition: Specifies the ID of the IPv6 subnet where the load balancer is located. This subnet is also called the frontend subnet. Range: N/A
ipv6_vip_port_id	String	Definition: Specifies the ID of the port bound to the IPv6 address of the load balancer. Range: N/A
availability_zone_list	Array of strings	Definition: Specifies the list of AZs where the load balancers are created. Range: N/A
enterprise_project_id	String	Definition: Specifies the ID of the enterprise project. Range: • 0: The resource belongs to the default enterprise project. • A string in UUID format indicates a non-default enterprise project.
billing_info	String	Definition: Provides resource billing information. Range: • If the value is left blank, the resource is billed on a pay-per-use basis. This parameter is unsupported. Please do not use it.
l4_flavor_id	String	Definition: Specifies the ID of a flavor at Layer 4. If the current load balancer is an elastic flavor instance, this parameter defines the maximum elastic flavor at Layer 4. Range: N/A

Parameter	Type	Description
l4_scale_flavor_id	String	Definition: Specifies the ID of an elastic flavor at Layer 4. Range: N/A NOTE This parameter has been discarded. Do not use it.
l7_flavor_id	String	Definition: Specifies the ID of a flavor at Layer 7. If the current load balancer is an elastic flavor instance, this parameter defines the maximum elastic flavor at Layer 7. Range: N/A
l7_scale_flavor_id	String	Definition: Specifies the ID of an elastic flavor at Layer 7. Range: N/A NOTE This parameter has been discarded. Do not use it.
gw_flavor_id	String	Definition: Specifies the flavor ID of the gateway load balancer. Range: N/A This parameter is unsupported. Please do not use it.
loadbalancer_type	String	Definition: Specifies the load balancer type. Range: gateway: gateway load balancers null: other types of load balancers This parameter is unsupported. Please do not use it.
publicips	Array of PublicIpInfo objects	Definition: Specifies the EIP bound to the load balancer. NOTE This parameter has the same meaning as eips .
global_eips	Array of GlobalEipInfo objects	Definition: Specifies the global EIP bound to the load balancer.
elb_virsubnet_ids	Array of strings	Definition: Specifies the network IDs of subnets on the downstream plane. Range: N/A

Parameter	Type	Description
elb_virsubnet_type	String	Definition: Specifies the type of the subnet on the downstream plane. Range: • ipv4: IPv4 subnets • dualstack: subnets that support IPv4/IPv6 dual stack
ip_target_enable	Boolean	Definition: Specifies whether to add backend servers that are not in the load balancer's VPC. 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. Range: • true: This option will be enabled. • false: This option will be disabled.
frozen_scene	String	Definition: Specifies the scenario where the load balancer is frozen. If there are multiple scenarios, separate them with commas (,). Range: • 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. • AREAR: The load balancer is frozen due to arrears.

Parameter	Type	Description
deletion_protection_enable	Boolean	Definition: Specifies whether to enable deletion protection. This parameter is returned only when the deletion protection is enabled in the current region. Range: • false: This option will be disabled. • true: This option will be enabled.
autoscaling	AutoscalingRef object	Definition: Specifies information about elastic scaling. If elastic scaling is enabled, the load balancer flavors can be automatically adjusted based on incoming traffic. NOTE 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 flavors will be created and you will be billed for the minimum flavors.
public_border_group	String	Definition: Specifies the public border group. Range: • center: public border group of the central site • Edge site name: public border group of an edge site
charge_mode	String	Definition: Specifies the charge mode of the load balancer. Range: • flavor: billed by the fixed flavor you select. • lcu: billed by how many LCUs you have used. • Null: If it is a shared load balancer, it is free. If it is a dedicated load balancer, it will be billed by the fixed flavor you select. This parameter is unsupported. Please do not use it.

Parameter	Type	Description
service_lb_mode	String	Definition: Specifies load balancer mode. Range: • lb: Cross-tenant access is not supported. • ep: Cross-tenant access is supported. This parameter is unsupported. Please do not use it.
instance_type	String	Definition: Specifies the internal service to which the load balancer belongs. Range: N/A This parameter is unsupported. Please do not use it.
instance_id	String	Definition: Specifies the ID of the instance with which the load balancer is associated. Range: N/A This parameter is unsupported. Please do not use it.
proxy_protocol_extensions	Array of ProxyProtocolExtension objects	Definition: Specifies the proxy protocol extension. This parameter is unsupported. Please do not use it.
waf_failure_action	String	Definition: Specifies traffic distributing policies when the WAF is faulty. Range: discard indicates traffic will not be distributed. forward indicates traffic will be distributed to the default backend servers.
protection_status	String	Definition: Specifies the protection status. Range: • nonProtection: The resource is not protected. • consoleProtection: Modification is not allowed on the console.

Parameter	Type	Description
protection_reason	String	Definition: Specifies why modification protection is enabled. Range: The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).
log_group_id	String	Definition: Specifies the ID of the log group that is associated with the load balancer. Range: N/A
log_topic_id	String	Definition: Specifies the ID of the log topic that is associated with the load balancer. Range: N/A
custom_qos_limit	CustomQosLimit object	Definition: Specifies the rate limit information of the ELB flavors. Range: N/A This parameter is unsupported. Please do not use it.

Table 5-121 PoolRef

Parameter	Type	Description
id	String	Definition: Specifies the backend server group ID. Range: N/A

Table 5-122 ListenerRef

Parameter	Type	Description
id	String	Definition: Specifies the listener ID. Range: N/A

Table 5-123 Tag

Parameter	Type	Description
key	String	Definition: Specifies the tag key. Range: N/A

Parameter	Type	Description
value	String	Definition: Specifies the tag value. Range: N/A

Table 5-124 EipInfo

Parameter	Type	Description
eip_id	String	Definition: Specifies the EIP ID. Range: N/A
eip_address	String	Definition: Specifies the EIP. Range: N/A
ip_version	Integer	Definition: Specifies the IP address version. Range: • 4: IPv4 addresses • 6: IPv6 addresses

Table 5-125 PublicIpInfo

Parameter	Type	Description
publicip_id	String	Definition: Specifies the EIP ID. Range: N/A
publicip_address	String	Definition: Specifies the EIP. Range: N/A
ip_version	Integer	Definition: Specifies the IP address version. Range: • 4: IPv4 address • 6: IPv6 address

Table 5-126 GlobalEipInfo

Parameter	Type	Description
global_eip_id	String	Definition: Specifies the ID of the global EIP. Range: N/A

Parameter	Type	Description
global_eip_addresses	String	Definition: Specifies the global EIP. Range: N/A
ip_version	Integer	Definition: Specifies the IP address version. Range: • 4: IPv4 addresses • 6: IPv6 addresses

Table 5-127 AutoscalingRef

Parameter	Type	Description
enable	Boolean	Definition: Specifies whether to enable elastic scaling for the load balancer. Range: • true: This option will be enabled. • false: This option will be disabled.
min_l7_flavor_id	String	Definition: Specifies the ID of the minimum elastic flavor at Layer 7. Range: N/A

Table 5-128 ProxyProtocolExtension

Parameter	Type	Description
vip_address	String	Definition: Specifies the IPv4 address. Constraints: N/A Range: N/A Default value: N/A
ipv6_vip_address	String	Definition: Specifies the IPv6 address. Constraints: N/A Range: N/A Default value: N/A
extension	Extension object	Definition: Specifies the proxy protocol extension. Constraints: N/A

Table 5-129 Extension

Parameter	Type	Description
ep_id	String	Definition: Specifies the VPC endpoint ID. Constraints: N/A Range: N/A Default value: N/A
ep_service_id	String	Definition: Specifies the VPC endpoint service ID. Constraints: N/A Range: N/A Default value: N/A

Table 5-130 CustomQosLimit

Parameter	Type	Description
l4	L4Limit object	Definition: Specifies the rate limit information of the ELB flavors at Layer 4.
l7	L7Limit object	Definition: Specifies the rate limit information of the ELB flavors at Layer 7.

Table 5-131 L4Limit

Parameter	Type	Description
connection	Integer	Definition: Specifies the maximum number of concurrent connections at Layer 4. Range: N/A
cps	Integer	Definition: Specifies the maximum number of new connections at Layer 4. Range: N/A

Table 5-132 L7Limit

Parameter	Type	Description
connection	Integer	Definition: Specifies the maximum number of concurrent connections at Layer 7. Range: N/A
cps	Integer	Definition: Specifies the maximum number of new connections at Layer 7. Range: N/A

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": "0aabc8aa8-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 huaweicloudskelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskelb.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 5-133 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
loadbalancer_id	Yes	String	Definition: Specifies the load balancer ID. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-134 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 204

Successful request.

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 huaweicloudskelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskelb.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 5-135 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
loadbalancer_id	Yes	String	Definition: Specifies the load balancer ID. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-136 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 204

Successful request.

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 huaweicloudskelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskelb.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	Successful request.

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 5-137 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
loadbalancer_id	Yes	String	Definition: Specifies the load balancer ID. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-138 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-139 Request body parameters

Parameter	Mandatory	Type	Description
loadbalancer	Yes	DeleteLoadBalancerCasca deOption object	Definition: Specifies the parameters for deleting a load balancer and its associated resources. Constraints: N/A

Table 5-140 DeleteLoadBalancerCascadeOption

Parameter	Mandatory	Type	Description
unbounded_pool	No	Boolean	Definition: Specifies whether to delete the associated backend server group. Constraints: - 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. Range: true: The backend server group will be deleted. false: The backend server group will be disassociated from the load balancer but not deleted. Default value: true
public_ip	No	Boolean	Definition: Specifies whether to release EIPs after the load balancer is deleted. Constraints: N/A Range: true: The EIPs will be released. false: The EIPs will be unbound from the load balancer but not released. Default value: false

Response Parameters

Status code: 204

Successful request.

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/delete-cascade  
  
{  
  "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	Successful request.

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, **DISABLE** 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 5-141 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
loadbalancer_id	Yes	String	Definition: Specifies the load balancer ID. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-142 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-143 Response body parameters

Parameter	Type	Description
statuses	LoadBalancerStatusResult object	Definition: Provides supplementary information about the load balancer status tree. Default value: N/A
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

Table 5-144 LoadBalancerStatusResult

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

Table 5-145 LoadBalancerStatus

Parameter	Type	Description
name	String	Definition: Specifies the load balancer name. Range: N/A

Parameter	Type	Description
provisioning_status	String	Definition: Specifies the provisioning status of the load balancer. Range: • ACTIVE: in use • PENDING_DELETE: deleting
listeners	Array of LoadBalancerStatusListener objects	Definition: Lists the listeners added to the load balancer.
pools	Array of LoadBalancerStatusPool objects	Definition: Lists the backend server groups associated with the load balancer.
id	String	Definition: Specifies the load balancer ID. Range: N/A
operating_status	String	Definition: Specifies the operating status of the load balancer. Range: • ONLINE: The load balancer is running normally. • FROZEN: The load balancer is frozen. • DEGRADED: This status is displayed only when operating_status is set to OFFLINE for a backend server associated with the load balancer. • DISABLED: This status is displayed only when admin_state_up of the 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 5-146 LoadBalancerStatusListener

Parameter	Type	Description
name	String	Definition: Specifies the name of the listener. Range: N/A

Parameter	Type	Description
provisioning_status	String	Definition: Specifies the provisioning status of the listener. Range: • ACTIVE: in use
pools	Array of LoadBalancerStatusPool objects	Definition: Specifies the operating status of the backend server groups associated with the listener.
l7policies	Array of LoadBalancerStatusPolicy objects	Definition: Specifies the operating status of the forwarding policy added to the listener.
id	String	Definition: Specifies the listener ID. Range: N/A
operating_status	String	Definition: Specifies the operating status of the listener. Range: • 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 5-147 LoadBalancerStatusPolicy

Parameter	Type	Description
action	String	Definition: Specifies whether requests are forwarded to another backend server group or redirected to an HTTPS listener. Range: • REDIRECT_TO_POOL: Requests are forwarded to another backend server group. • REDIRECT_TO_LISTENER: Requests are redirected to an HTTPS listener.
id	String	Definition: Specifies the forwarding policy ID. Range: N/A
provisioning_status	String	Definition: Specifies the provisioning status of the forwarding policy. Range: • ACTIVE (default): The forwarding policy is provisioned successfully. • ERROR: The forwarding policy has the same rule as another forwarding policy added to the same listener.
name	String	Definition: Specifies the forwarding policy name. Range: N/A
rules	Array of LoadBalancerStatusL7Rule objects	Definition: Specifies the status of all forwarding rules in the forwarding policy.

Table 5-148 LoadBalancerStatusL7Rule

Parameter	Type	Description
id	String	Definition: Specifies the ID of the forwarding rule. Range: N/A

Parameter	Type	Description
type	String	Definition: Specifies the type of the match content. Range: • HOST_NAME: A domain name will be used for matching. • PATH: A URL will be used for matching.
provisioning_status	String	Definition: Specifies the provisioning status of the forwarding rule. Range: • ACTIVE (default): The forwarding rule is in use. • ERROR: The forwarding policy has the same rule as another forwarding policy added to the same listener.

Table 5-149 LoadBalancerStatusPool

Parameter	Type	Description
provisioning_status	String	Definition: Specifies the provisioning status of the backend server group. Range: • ACTIVE: in use
name	String	Definition: Specifies the backend server group name. Range: N/A
healthmonitor	LoadBalancerStatusHealthMonitor object	Definition: Specifies the health check results of backend servers in the load balancer status tree.
members	Array of LoadBalancerStatusMember objects	Definition: Specifies the statuses of all backend servers in the backend server group.
id	String	Definition: Specifies the backend server group ID. Range: N/A

Parameter	Type	Description
operating_status	String	Definition: Specifies the operating status of the backend server group. Range: • 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 5-150 LoadBalancerStatusHealthMonitor

Parameter	Type	Description
type	String	Definition: Specifies the health check protocol. Range: TCP, UDP_CONNECT, or HTTP.
id	String	Definition: Specifies the health check ID. Range: N/A
name	String	Definition: Specifies the health check name. Range: N/A
provisioning_status	String	Definition: Specifies the provisioning status of the health check. Range: The value can only be ACTIVE , indicating that the health check is in use.

Table 5-151 LoadBalancerStatusMember

Parameter	Type	Description
provisioning_status	String	Definition: Specifies the provisioning status of the backend server. Range: The value can only be ACTIVE , indicating that the backend server is in use.
address	String	Definition: Specifies the IP address of the backend server. Range: N/A
protocol_port	Integer	Definition: Specifies the port used by the backend server to receive requests. Range: 1 to 65535
id	String	Definition: Specifies the backend server ID. Range: N/A
operating_status	String	Definition: Specifies the operating status of the backend server. Range: • 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 Querying the Ports on the Downstream Subnet Used by a Load Balancer

Function

This API is used to query the ports and IP addresses on the downstream subnet used by a load balancer to forward requests within a private network.

Calling Method

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

URI

GET /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}/local-ports

Table 5-152 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Parameter	Mandatory	Type	Description
loadbalancer_id	Yes	String	Definition: Specifies the load balancer ID. Constraints: N/A Range: N/A Default value: N/A

Table 5-153 Query Parameters

Parameter	Mandatory	Type	Description
port_id	No	Array of strings	Definition: Specifies the ID of the port used by the load balancer. Multiple IDs can be used for query in the format of <i>port_id=xxx&port_id=xxx</i> .
ip_address	No	Array of strings	Definition: Specifies the private IPv4 address used by the load balancer. Constraints: N/A Range: N/A Default value: N/A Multiple IP addresses can be used for query in the format of <i>ip_address=xxx&ip_address=xxx</i> .
ipv6_address	No	Array of strings	Definition: Specifies the IPv6 address used by the load balancer. Constraints: N/A Range: N/A Default value: N/A Multiple IPv6 addresses can be used for query in the format of <i>ipv6_address=xxx&ipv6_addresses=xxx</i> .

Parameter	Mandatory	Type	Description
type	No	Array of strings	Definition: Specifies the port type. Constraints: N/A Range: N/A Default value: N/A Multiple types can be used for query in the format of <i>type=xxx&type=xxx</i> .
virsubnet_id	No	Array of strings	Definition: Specifies the network ID of the downstream subnet where the port is located. Constraints: N/A Range: N/A Default value: N/A Multiple IDs can be used for query in the format of <i>virsubnet_id=xxx&virsubnet_id=xxx</i> .

Request Parameters

Table 5-154 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-155 Response body parameters

Parameter	Type	Description
ports	Array of LocalPort objects	Definition: Specifies the ports used by the load balancer.

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

Table 5-156 LocalPort

Parameter	Type	Description
port_id	String	Definition: Specifies the ID of the port used by the load balancer. Range: N/A
ip_address	String	Definition: Specifies the private IPv4 address used by the load balancer. Range: N/A
ipv6_address	String	Definition: Specifies the IPv6 address used by the load balancer. Range: N/A
type	String	Definition: Specifies the port type. Range: • l4_hc: port used for health checks during Layer 4 traffic forwarding using DNAT. • l4: port used for Layer 4 health checks and traffic forwarding using FullNAT. • l7: port used for Layer 7 health checks and service forwarding.
virsubnet_id	String	Definition: Specifies the network ID of the downstream subnet where the port is located. Range: N/A

Example Requests

Querying the ports used by a load balancer

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


Example Responses

Status code: 200

Successful operation

```
{
  "ports": [ {
    "port_id": "b796e55e-988a-429e-a132-9245beb046e5",
    "ip_address": "192.168.1.2",
    "ipv6_address": "2420:2023:410:151:49c:7163:342a:3e3",
    "type": "l4_hc",
    "virsubnet_id": "4507af92-719f-4878-9394-6a6a6ba1dcbb"
  } ]
}
```

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 ShowLoadBalancerPortsSolution {

    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();
        ShowLoadBalancerPortsRequest request = new ShowLoadBalancerPortsRequest();
        request.withLoadbalancerId("{loadbalancer_id}");
        try {
            ShowLoadBalancerPortsResponse response = client.showLoadBalancerPorts(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 huaweicloudskelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskelb.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 = ShowLoadBalancerPortsRequest()
        request.loadbalancer_id = "{loadbalancer_id}"
        response = client.show_load_balancer_ports(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.ShowLoadBalancerPortsRequest{}
request.LoadbalancerId = "{loadbalancer_id}"
response, err := client.ShowLoadBalancerPorts(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 operation

Error Codes

See [Error Codes](#).

5.6.13 Deploying a Load Balancer in Additional AZs

Function

This API is used to deploy a load balancer in additional AZs.

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 5-157 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
loadbalancer_id	Yes	String	Definition: Specifies the load balancer ID. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-158 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-159 Request body parameters

Parameter	Mandatory	Type	Description
availability_zone_list	Yes	Array of strings	Definition: Specifies new AZs where the load balancer will be deployed. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-160 Response body parameters

Parameter	Type	Description
loadbalancer	LoadBalancer object	Definition: Specifies the load balancer.
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

Table 5-161 LoadBalancer

Parameter	Type	Description
id	String	Definition: Specifies the load balancer ID. Range: N/A
description	String	Definition: Provides supplementary information about the load balancer. Range: N/A
provisioning_status	String	Definition: Specifies the provisioning status of the load balancer. Range: • ACTIVE: in use • PENDING_DELETE: deleting
admin_state_up	Boolean	Definition: Specifies whether the load balancer is enabled. Range: • true: enabled • false: disabled
provider	String	Definition: Specifies the provider of the load balancer. The value is fixed to vlb . Range: N/A
pools	Array of PoolRef objects	Definition: Lists the IDs of backend server groups associated with the load balancer.

Parameter	Type	Description
listeners	Array of ListenerRef objects	Definition: Lists the IDs of listeners associated with the load balancer.
operating_status	String	Definition: Specifies the operating status of the load balancer. Range: • ONLINE: The load balancer is online. • FROZEN: The load balancer is frozen.
name	String	Definition: Specifies the load balancer name. Range: N/A
project_id	String	Definition: Specifies the ID of the project where the load balancer is used. Range: N/A
vip_subnet_cidr_id	String	Definition: Specifies the ID of the IPv4 subnet where the load balancer is located. This subnet is also called the frontend subnet. Range: N/A
vip_address	String	Definition: Specifies the private IPv4 address of the load balancer. Range: N/A
vip_port_id	String	Definition: Specifies the ID of the port bound to the private IPv4 address of the load balancer. Range: N/A
tags	Array of Tag objects	Definition: Specifies the tags added to the load balancer.
created_at	String	Definition: Specifies the time when the load balancer was created. Range: The value must be in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> .

Parameter	Type	Description
updated_at	String	Definition: Specifies the time when the load balancer was updated. Range: The value must be in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> .
guaranteed	Boolean	Definition: Specifies whether the load balancer is a dedicated load balancer. Range: • false: The load balancer is a shared load balancer. • true: The load balancer is a dedicated load balancer.
vpc_id	String	Definition: Specifies the ID of the VPC where the load balancer is located. Range: N/A
eips	Array of EipInfo objects	Definition: Specifies the EIP bound to the load balancer. NOTE This parameter has the same meaning as publicips .
ipv6_vip_address	String	Definition: Specifies the IPv6 address of the load balancer. Range: N/A
ipv6_vip_virsubnet_id	String	Definition: Specifies the ID of the IPv6 subnet where the load balancer is located. This subnet is also called the frontend subnet. Range: N/A
ipv6_vip_port_id	String	Definition: Specifies the ID of the port bound to the IPv6 address of the load balancer. Range: N/A
availability_zone_list	Array of strings	Definition: Specifies the list of AZs where the load balancers are created. Range: N/A

Parameter	Type	Description
enterprise_project_id	String	Definition: Specifies the ID of the enterprise project. Range: • 0: The resource belongs to the default enterprise project. • A string in UUID format indicates a non-default enterprise project.
billing_info	String	Definition: Provides resource billing information. Range: • If the value is left blank, the resource is billed on a pay-per-use basis. This parameter is unsupported. Please do not use it.
l4_flavor_id	String	Definition: Specifies the ID of a flavor at Layer 4. If the current load balancer is an elastic flavor instance, this parameter defines the maximum elastic flavor at Layer 4. Range: N/A
l4_scale_flavor_id	String	Definition: Specifies the ID of an elastic flavor at Layer 4. Range: N/A NOTE This parameter has been discarded. Do not use it.
l7_flavor_id	String	Definition: Specifies the ID of a flavor at Layer 7. If the current load balancer is an elastic flavor instance, this parameter defines the maximum elastic flavor at Layer 7. Range: N/A
l7_scale_flavor_id	String	Definition: Specifies the ID of an elastic flavor at Layer 7. Range: N/A NOTE This parameter has been discarded. Do not use it.

Parameter	Type	Description
gw_flavor_id	String	Definition: Specifies the flavor ID of the gateway load balancer. Range: N/A This parameter is unsupported. Please do not use it.
loadbalancer_type	String	Definition: Specifies the load balancer type. Range: • gateway: gateway load balancers • null: other types of load balancers This parameter is unsupported. Please do not use it.
publicips	Array of PublicIpInfo objects	Definition: Specifies the EIP bound to the load balancer. NOTE This parameter has the same meaning as eips .
global_eips	Array of GlobalEipInfo objects	Definition: Specifies the global EIP bound to the load balancer.
elb_virsubnet_ids	Array of strings	Definition: Specifies the network IDs of subnets on the downstream plane. Range: N/A
elb_virsubnet_type	String	Definition: Specifies the type of the subnet on the downstream plane. Range: • ipv4: IPv4 subnets • dualstack: subnets that support IPv4/IPv6 dual stack

Parameter	Type	Description
ip_target_enable	Boolean	Definition: Specifies whether to add backend servers that are not in the load balancer's VPC. 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. Range: • true: This option will be enabled. • false: This option will be disabled.
frozen_scene	String	Definition: Specifies the scenario where the load balancer is frozen. If there are multiple scenarios, separate them with commas (,). Range: • 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. • AREAR: The load balancer is frozen due to arrears.
deletion_protection_enable	Boolean	Definition: Specifies whether to enable deletion protection. This parameter is returned only when the deletion protection is enabled in the current region. Range: • false: This option will be disabled. • true: This option will be enabled.

Parameter	Type	Description
autoscaling	AutoscalingRef object	Definition: Specifies information about elastic scaling. If elastic scaling is enabled, the load balancer flavors can be automatically adjusted based on incoming traffic. NOTE 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 flavors will be created and you will be billed for the minimum flavors.
public_border_group	String	Definition: Specifies the public border group. Range: • center: public border group of the central site • Edge site name: public border group of an edge site
charge_mode	String	Definition: Specifies the charge mode of the load balancer. Range: • flavor: billed by the fixed flavor you select. • lcu: billed by how many LCUs you have used. • Null: If it is a shared load balancer, it is free. If it is a dedicated load balancer, it will be billed by the fixed flavor you select. This parameter is unsupported. Please do not use it.
service_lb_mode	String	Definition: Specifies load balancer mode. Range: • lb: Cross-tenant access is not supported. • ep: Cross-tenant access is supported. This parameter is unsupported. Please do not use it.

Parameter	Type	Description
instance_type	String	Definition: Specifies the internal service to which the load balancer belongs. Range: N/A This parameter is unsupported. Please do not use it.
instance_id	String	Definition: Specifies the ID of the instance with which the load balancer is associated. Range: N/A This parameter is unsupported. Please do not use it.
proxy_protocol_extensions	Array of ProxyProtocolExtension objects	Definition: Specifies the proxy protocol extension. This parameter is unsupported. Please do not use it.
waf_failure_action	String	Definition: Specifies traffic distributing policies when the WAF is faulty. Range: discard indicates traffic will not be distributed. forward indicates traffic will be distributed to the default backend servers.
protection_status	String	Definition: Specifies the protection status. Range: • nonProtection: The resource is not protected. • consoleProtection: Modification is not allowed on the console.
protection_reason	String	Definition: Specifies why modification protection is enabled. Range: The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).
log_group_id	String	Definition: Specifies the ID of the log group that is associated with the load balancer. Range: N/A
log_topic_id	String	Definition: Specifies the ID of the log topic that is associated with the load balancer. Range: N/A

Parameter	Type	Description
custom_qos_limit	CustomQosLimit object	Definition: Specifies the rate limit information of the ELB flavors. Range: N/A This parameter is unsupported. Please do not use it.

Table 5-162 PoolRef

Parameter	Type	Description
id	String	Definition: Specifies the backend server group ID. Range: N/A

Table 5-163 ListenerRef

Parameter	Type	Description
id	String	Definition: Specifies the listener ID. Range: N/A

Table 5-164 Tag

Parameter	Type	Description
key	String	Definition: Specifies the tag key. Range: N/A
value	String	Definition: Specifies the tag value. Range: N/A

Table 5-165 EipInfo

Parameter	Type	Description
eip_id	String	Definition: Specifies the EIP ID. Range: N/A
eip_address	String	Definition: Specifies the EIP. Range: N/A

Parameter	Type	Description
ip_version	Integer	Definition: Specifies the IP address version. Range: • 4: IPv4 addresses • 6: IPv6 addresses

Table 5-166 PublicIpInfo

Parameter	Type	Description
publicip_id	String	Definition: Specifies the EIP ID. Range: N/A
publicip_address	String	Definition: Specifies the EIP. Range: N/A
ip_version	Integer	Definition: Specifies the IP address version. Range: • 4: IPv4 address • 6: IPv6 address

Table 5-167 GlobalEipInfo

Parameter	Type	Description
global_eip_id	String	Definition: Specifies the ID of the global EIP. Range: N/A
global_eip_addresses	String	Definition: Specifies the global EIP. Range: N/A
ip_version	Integer	Definition: Specifies the IP address version. Range: • 4: IPv4 addresses • 6: IPv6 addresses

Table 5-168 AutoscalingRef

Parameter	Type	Description
enable	Boolean	Definition: Specifies whether to enable elastic scaling for the load balancer. Range: • true: This option will be enabled. • false: This option will be disabled.
min_l7_flavor_id	String	Definition: Specifies the ID of the minimum elastic flavor at Layer 7. Range: N/A

Table 5-169 ProxyProtocolExtension

Parameter	Type	Description
vip_address	String	Definition: Specifies the IPv4 address. Constraints: N/A Range: N/A Default value: N/A
ipv6_vip_address	String	Definition: Specifies the IPv6 address. Constraints: N/A Range: N/A Default value: N/A
extension	Extension object	Definition: Specifies the proxy protocol extension. Constraints: N/A

Table 5-170 Extension

Parameter	Type	Description
ep_id	String	Definition: Specifies the VPC endpoint ID. Constraints: N/A Range: N/A Default value: N/A

Parameter	Type	Description
ep_service_id	String	Definition: Specifies the VPC endpoint service ID. Constraints: N/A Range: N/A Default value: N/A

Table 5-171 CustomQosLimit

Parameter	Type	Description
l4	L4Limit object	Definition: Specifies the rate limit information of the ELB flavors at Layer 4.
l7	L7Limit object	Definition: Specifies the rate limit information of the ELB flavors at Layer 7.

Table 5-172 L4Limit

Parameter	Type	Description
connection	Integer	Definition: Specifies the maximum number of concurrent connections at Layer 4. Range: N/A
cps	Integer	Definition: Specifies the maximum number of new connections at Layer 4. Range: N/A

Table 5-173 L7Limit

Parameter	Type	Description
connection	Integer	Definition: Specifies the maximum number of concurrent connections at Layer 7. Range: N/A
cps	Integer	Definition: Specifies the maximum number of new connections at Layer 7. Range: N/A

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

Successful request.

```
{  
  "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	Successful request.

Error Codes

See [Error Codes](#).

5.6.14 Removing a Load Balancer from AZs

Function

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

 NOTE

Removing a load balancer from an AZ may disconnect existing connections.

Constraints

- This API is only available for dedicated load balancers.
- You cannot remove a load balancer from all AZs where it is working.

Calling Method

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

URI

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

Table 5-174 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
loadbalancer_id	Yes	String	Definition: Specifies the load balancer ID. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-175 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-176 Request body parameters

Parameter	Mandatory	Type	Description
availability_zone_list	Yes	Array of strings	Definition: Specifies the AZs where the load balancer will be removed. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-177 Response body parameters

Parameter	Type	Description
loadbalancer	LoadBalancer object	Definition: Specifies the load balancer.
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

Table 5-178 LoadBalancer

Parameter	Type	Description
id	String	Definition: Specifies the load balancer ID. Range: N/A
description	String	Definition: Provides supplementary information about the load balancer. Range: N/A
provisioning_status	String	Definition: Specifies the provisioning status of the load balancer. Range: • ACTIVE: in use • PENDING_DELETE: deleting
admin_state_up	Boolean	Definition: Specifies whether the load balancer is enabled. Range: • true: enabled • false: disabled
provider	String	Definition: Specifies the provider of the load balancer. The value is fixed to vlb . Range: N/A
pools	Array of PoolRef objects	Definition: Lists the IDs of backend server groups associated with the load balancer.
listeners	Array of ListenerRef objects	Definition: Lists the IDs of listeners associated with the load balancer.
operating_status	String	Definition: Specifies the operating status of the load balancer. Range: • ONLINE: The load balancer is online. • FROZEN: The load balancer is frozen.
name	String	Definition: Specifies the load balancer name. Range: N/A

Parameter	Type	Description
project_id	String	Definition: Specifies the ID of the project where the load balancer is used. Range: N/A
vip_subnet_cidr_id	String	Definition: Specifies the ID of the IPv4 subnet where the load balancer is located. This subnet is also called the frontend subnet. Range: N/A
vip_address	String	Definition: Specifies the private IPv4 address of the load balancer. Range: N/A
vip_port_id	String	Definition: Specifies the ID of the port bound to the private IPv4 address of the load balancer. Range: N/A
tags	Array of Tag objects	Definition: Specifies the tags added to the load balancer.
created_at	String	Definition: Specifies the time when the load balancer was created. Range: The value must be in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> .
updated_at	String	Definition: Specifies the time when the load balancer was updated. Range: The value must be in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> .
guaranteed	Boolean	Definition: Specifies whether the load balancer is a dedicated load balancer. Range: • false: The load balancer is a shared load balancer. • true: The load balancer is a dedicated load balancer.
vpc_id	String	Definition: Specifies the ID of the VPC where the load balancer is located. Range: N/A

Parameter	Type	Description
eips	Array of EipInfo objects	Definition: Specifies the EIP bound to the load balancer. NOTE This parameter has the same meaning as publicips .
ipv6_vip_address	String	Definition: Specifies the IPv6 address of the load balancer. Range: N/A
ipv6_vip_virsubnet_id	String	Definition: Specifies the ID of the IPv6 subnet where the load balancer is located. This subnet is also called the frontend subnet. Range: N/A
ipv6_vip_port_id	String	Definition: Specifies the ID of the port bound to the IPv6 address of the load balancer. Range: N/A
availability_zone_list	Array of strings	Definition: Specifies the list of AZs where the load balancers are created. Range: N/A
enterprise_project_id	String	Definition: Specifies the ID of the enterprise project. Range: • 0: The resource belongs to the default enterprise project. • A string in UUID format indicates a non-default enterprise project.
billing_info	String	Definition: Provides resource billing information. Range: • If the value is left blank, the resource is billed on a pay-per-use basis. This parameter is unsupported. Please do not use it.
l4_flavor_id	String	Definition: Specifies the ID of a flavor at Layer 4. If the current load balancer is an elastic flavor instance, this parameter defines the maximum elastic flavor at Layer 4. Range: N/A

Parameter	Type	Description
l4_scale_flavor_id	String	Definition: Specifies the ID of an elastic flavor at Layer 4. Range: N/A NOTE This parameter has been discarded. Do not use it.
l7_flavor_id	String	Definition: Specifies the ID of a flavor at Layer 7. If the current load balancer is an elastic flavor instance, this parameter defines the maximum elastic flavor at Layer 7. Range: N/A
l7_scale_flavor_id	String	Definition: Specifies the ID of an elastic flavor at Layer 7. Range: N/A NOTE This parameter has been discarded. Do not use it.
gw_flavor_id	String	Definition: Specifies the flavor ID of the gateway load balancer. Range: N/A This parameter is unsupported. Please do not use it.
loadbalancer_type	String	Definition: Specifies the load balancer type. Range: • gateway: gateway load balancers • null: other types of load balancers This parameter is unsupported. Please do not use it.
publicips	Array of PublicIpInfo objects	Definition: Specifies the EIP bound to the load balancer. NOTE This parameter has the same meaning as eips .
global_eips	Array of GlobalEipInfo objects	Definition: Specifies the global EIP bound to the load balancer.
elb_virsubnet_ids	Array of strings	Definition: Specifies the network IDs of subnets on the downstream plane. Range: N/A

Parameter	Type	Description
elb_virsubnet_type	String	Definition: Specifies the type of the subnet on the downstream plane. Range: • ipv4: IPv4 subnets • dualstack: subnets that support IPv4/IPv6 dual stack
ip_target_enable	Boolean	Definition: Specifies whether to add backend servers that are not in the load balancer's VPC. 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. Range: • true: This option will be enabled. • false: This option will be disabled.
frozen_scene	String	Definition: Specifies the scenario where the load balancer is frozen. If there are multiple scenarios, separate them with commas (,). Range: • 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. • AREAR: The load balancer is frozen due to arrears.

Parameter	Type	Description
deletion_protection_enable	Boolean	Definition: Specifies whether to enable deletion protection. This parameter is returned only when the deletion protection is enabled in the current region. Range: • false: This option will be disabled. • true: This option will be enabled.
autoscaling	AutoscalingRef object	Definition: Specifies information about elastic scaling. If elastic scaling is enabled, the load balancer flavors can be automatically adjusted based on incoming traffic. NOTE 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 flavors will be created and you will be billed for the minimum flavors.
public_border_group	String	Definition: Specifies the public border group. Range: • center: public border group of the central site • Edge site name: public border group of an edge site
charge_mode	String	Definition: Specifies the charge mode of the load balancer. Range: • flavor: billed by the fixed flavor you select. • lcu: billed by how many LCUs you have used. • Null: If it is a shared load balancer, it is free. If it is a dedicated load balancer, it will be billed by the fixed flavor you select. This parameter is unsupported. Please do not use it.

Parameter	Type	Description
service_lb_mode	String	Definition: Specifies load balancer mode. Range: • lb: Cross-tenant access is not supported. • ep: Cross-tenant access is supported. This parameter is unsupported. Please do not use it.
instance_type	String	Definition: Specifies the internal service to which the load balancer belongs. Range: N/A This parameter is unsupported. Please do not use it.
instance_id	String	Definition: Specifies the ID of the instance with which the load balancer is associated. Range: N/A This parameter is unsupported. Please do not use it.
proxy_protocol_extensions	Array of ProxyProtocolExtension objects	Definition: Specifies the proxy protocol extension. This parameter is unsupported. Please do not use it.
waf_failure_action	String	Definition: Specifies traffic distributing policies when the WAF is faulty. Range: discard indicates traffic will not be distributed. forward indicates traffic will be distributed to the default backend servers.
protection_status	String	Definition: Specifies the protection status. Range: • nonProtection: The resource is not protected. • consoleProtection: Modification is not allowed on the console.

Parameter	Type	Description
protection_reason	String	Definition: Specifies why modification protection is enabled. Range: The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).
log_group_id	String	Definition: Specifies the ID of the log group that is associated with the load balancer. Range: N/A
log_topic_id	String	Definition: Specifies the ID of the log topic that is associated with the load balancer. Range: N/A
custom_qos_limit	CustomQosLimit object	Definition: Specifies the rate limit information of the ELB flavors. Range: N/A This parameter is unsupported. Please do not use it.

Table 5-179 PoolRef

Parameter	Type	Description
id	String	Definition: Specifies the backend server group ID. Range: N/A

Table 5-180 ListenerRef

Parameter	Type	Description
id	String	Definition: Specifies the listener ID. Range: N/A

Table 5-181 Tag

Parameter	Type	Description
key	String	Definition: Specifies the tag key. Range: N/A

Parameter	Type	Description
value	String	Definition: Specifies the tag value. Range: N/A

Table 5-182 EipInfo

Parameter	Type	Description
eip_id	String	Definition: Specifies the EIP ID. Range: N/A
eip_address	String	Definition: Specifies the EIP. Range: N/A
ip_version	Integer	Definition: Specifies the IP address version. Range: • 4: IPv4 addresses • 6: IPv6 addresses

Table 5-183 PublicIpInfo

Parameter	Type	Description
publicip_id	String	Definition: Specifies the EIP ID. Range: N/A
publicip_address	String	Definition: Specifies the EIP. Range: N/A
ip_version	Integer	Definition: Specifies the IP address version. Range: • 4: IPv4 address • 6: IPv6 address

Table 5-184 GlobalEipInfo

Parameter	Type	Description
global_eip_id	String	Definition: Specifies the ID of the global EIP. Range: N/A

Parameter	Type	Description
global_eip_addresses	String	Definition: Specifies the global EIP. Range: N/A
ip_version	Integer	Definition: Specifies the IP address version. Range: • 4: IPv4 addresses • 6: IPv6 addresses

Table 5-185 AutoscalingRef

Parameter	Type	Description
enable	Boolean	Definition: Specifies whether to enable elastic scaling for the load balancer. Range: • true: This option will be enabled. • false: This option will be disabled.
min_l7_flavor_id	String	Definition: Specifies the ID of the minimum elastic flavor at Layer 7. Range: N/A

Table 5-186 ProxyProtocolExtension

Parameter	Type	Description
vip_address	String	Definition: Specifies the IPv4 address. Constraints: N/A Range: N/A Default value: N/A
ipv6_vip_address	String	Definition: Specifies the IPv6 address. Constraints: N/A Range: N/A Default value: N/A
extension	Extension object	Definition: Specifies the proxy protocol extension. Constraints: N/A

Table 5-187 Extension

Parameter	Type	Description
ep_id	String	Definition: Specifies the VPC endpoint ID. Constraints: N/A Range: N/A Default value: N/A
ep_service_id	String	Definition: Specifies the VPC endpoint service ID. Constraints: N/A Range: N/A Default value: N/A

Table 5-188 CustomQosLimit

Parameter	Type	Description
l4	L4Limit object	Definition: Specifies the rate limit information of the ELB flavors at Layer 4.
l7	L7Limit object	Definition: Specifies the rate limit information of the ELB flavors at Layer 7.

Table 5-189 L4Limit

Parameter	Type	Description
connection	Integer	Definition: Specifies the maximum number of concurrent connections at Layer 4. Range: N/A
cps	Integer	Definition: Specifies the maximum number of new connections at Layer 4. Range: N/A

Table 5-190 L7Limit

Parameter	Type	Description
connection	Integer	Definition: Specifies the maximum number of concurrent connections at Layer 7. Range: N/A
cps	Integer	Definition: Specifies the maximum number of new connections at Layer 7. Range: N/A

Example Requests

Removing a load balancer from AZs

```
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

Successful request.

```
{  
  "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_virusubnet_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_virusubnet_ids" : [ "7f817f9c-8731-4002-9e47-18cb8d431787" ],  
    "elb_virusubnet_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 a load balancer from AZs

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

Python

Removing a load balancer from AZs

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudskelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskelb.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 a load balancer from AZs

```
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	Successful request.

Error Codes

See [Error Codes](#).

5.7 Certificate

5.7.1 Creating a Certificate

Function

This API is used to add a certificate for an HTTPS, TLS, or QUIC listener. You can associate a certificate from Cloud Certificate Manager (CCM) or use your own certificate.

Calling Method

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

URI

POST /v3/{project_id}/elb/certificates

Table 5-191 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-192 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-193 Request body parameters

Parameter	Mandatory	Type	Description
certificate	Yes	CreateCertificateOption object	Definition: Specifies the parameters for creating a certificate. Constraints: N/A

Table 5-194 CreateCertificateOption

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Definition: Specifies the administrative status of the certificate. This parameter does not take effect whether it is set to true or false . Constraints: N/A Range: • true: The certificate is available. • false: The certificate is unavailable. Default value: true

Parameter	Mandatory	Type	Description
certificate	No	String	Definition: Specifies the certificate content. It supports certificate chains with a maximum of 11 layers (including certificates and certificate chains). Constraints: N/A Range: The value must be PEM encoded, and can contain a maximum of 65,536 characters. Default value: N/A
description	No	String	Definition: Provides supplementary information about the certificate. Constraints: N/A Range: 0 to 255 characters. Default value: N/A

Parameter	Mandatory	Type	Description
domain	No	String	Definition: Specifies the domain names used by the server certificate. Constraints: This parameter will take effect only when type is set to server. (For other types of certificates, this parameter can be specified but does not take effect.) Range: 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 Default value: N/A
name	No	String	Definition: Specifies the certificate name. Constraints: N/A Range: 0 to 255 characters. Default value: N/A

Parameter	Mandatory	Type	Description
private_key	No	String	Definition: Specifies the private key of the server certificate. Constraints: • This parameter is valid and mandatory only when type is set to server or server_sm. • This parameter will be ignored if type is set to other values. The value must be PEM encoded and will not take effect. Range: The value must be PEM encoded, and can contain a maximum of 8,192 characters. Default value: N/A
project_id	No	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID. Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A NOTE This parameter is invalid. The project ID in the URL is used.
type	No	String	Definition: Specifies the certificate type. Constraints: N/A Range: • server: server certificates • client CA certificates • server_sm: server SM certificates Default value: server

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Definition: Specifies the ID of the enterprise project. If no enterprise project ID is specified during resource creation, 0 is returned, indicating that the resource belongs to the default enterprise project. Constraints: The enterprise project ID cannot be "", 0, or an enterprise project ID that does not exist. Range: N/A Default value: 0
enc_certificate	No	String	Definition: Specifies the content of the server SM certificate. It supports certificate chains with a maximum of 11 layers (including certificates and certificate chains). Constraints: This parameter is supported and mandatory only when type is set to server_sm . Range: The value must be PEM encoded, and can contain a maximum of 65,536 characters. Default value: N/A
enc_private_key	No	String	Definition: Specifies the private key of the server SM certificate. Constraints: This parameter is supported and mandatory only when type is set to server_sm . Range: The value must be PEM encoded, and can contain a maximum of 8,192 characters. Default value: N/A

Parameter	Mandatory	Type	Description
scm_certificate_id	No	String	Definition: Specifies the ID of the certificate managed on Cloud Certificate Manager (CCM). Constraints: The system records only the certificate ID but does not verify its existence on CCM. In addition, you need to update the content of the corresponding certificate on CCM to the related parameters (certificate , private_key , enc_certificate , and enc_private_key) of the current API. Range: N/A Default value: N/A
source	No	String	Definition: Specifies the source of the certificate. Constraints: none Range: • scm: certificates from CCM • Empty: self-signed certificates Default value: scm if scm_certificate_id is not empty. Otherwise, this parameter is left blank by default.
protection_status	No	String	Definition: Specifies the protection status. Constraints: N/A Range: • nonProtection: The resource is not protected. • consoleProtection: Modification is not allowed on the console. Default value: nonProtection

Parameter	Mandatory	Type	Description
protection_reason	No	String	Definition: Specifies why modification protection is enabled. Constraints: This parameter is valid only when protection_status is set to consoleProtection . Range: N/A Default value: N/A

Response Parameters

Status code: 201

Table 5-195 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
certificate	CertificateInfo object	Definition: ELB certificate information. The certificate is defined by the sub-parameter.

Table 5-196 CertificateInfo

Parameter	Type	Description
admin_state_up	Boolean	Definition: Specifies the administrative status of the certificate. This parameter does not take effect whether it is set to true or false . Range: true: The certificate is available. false: The certificate is unavailable.

Parameter	Type	Description
certificate	String	Definition: Specifies the certificate content. It supports certificate chains with a maximum of 11 layers (including certificates and certificate chains). Range: The value must be PEM encoded, and can contain a maximum of 65,536 characters.
description	String	Definition: Provides supplementary information about the certificate. Range: 0 to 255 characters.
domain	String	Definition: Specifies the domain names used by the server certificate. Range: 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	Definition: Specifies the certificate ID. Range: The value consists of 32 digits and lowercase letters.
name	String	Definition: Specifies the certificate name. Range: 0 to 255 characters.
private_key	String	Definition: Specifies the private key of the server certificate. Range: The value must be PEM encoded, and can contain a maximum of 8,192 characters.

Parameter	Type	Description
type	String	Definition: Specifies the certificate type. Range: • server: server certificates • client CA certificates • server_sm: server SM certificates
created_at	String	Definition: Specifies the creation time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.
updated_at	String	Definition: Specifies the update time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.
expire_time	String	Definition: Specifies the time when the certificate expires. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.
project_id	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Range: The value can contain a maximum of 32 characters, including digits and lowercase letters.
enc_certificate	String	Definition: Specifies the content of the server SM certificate. It supports certificate chains with a maximum of 11 layers (including certificates and certificate chains). Range: The value must be PEM encoded, and can contain a maximum of 65536 characters.
enc_private_key	String	Definition: Specifies the private key of the server SM certificate. Range: The value must be PEM encoded, and can contain a maximum of 8,192 characters.
scm_certificate_id	String	Definition: Specifies the ID of the certificate managed on Cloud Certificate Manager (CCM). Range: N/A

Parameter	Type	Description
common_name	String	Definition: Specifies the primary domain name of the certificate. Range: N/A
fingerprint	String	Definition: Specifies the fingerprint of the certificate. Range: N/A
subject_alternative_names	Array of strings	Definition: Specifies all the domain names of the certificate. Range: N/A
source	String	Definition: Specifies the source of the certificate. Range: • scm: certificates from CCM • Empty: self-signed certificates
protection_status	String	Definition: Specifies the protection status. Range: • nonProtection: The resource is not protected. • consoleProtection: Modification is not allowed on the console.
protection_reason	String	Definition: Specifies why modification protection is enabled. Range: N/A

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-----
\nMIIIEvgIBADANBgkqhkiG9w0BAQEFAASCBAgEAAoIBAQDQVAbOLe5xNf4M
\n253Wn9vhdUzojetjv4J+B7kYwsMhRcgdcJ8KCnX1nfzTvi2ksXLTQ2o9BkpStnPe\ntB4s32ZiJRMlk
+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM
\nMD30gLh6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8lcq39buNplgDOWzEP5AqzXt
\nCOFYn6RTH5SRug4hKNN7sT1eYMsIHu7wtEBDKVgrLjOCe/W2f8rLT1zEsoAW2Chl\nZAPYUBkl/
OXuTWRg3CohPPcl+UtlRSfvLDeeQ460swjbgwS/RbJh3slwLCRLU08k\nEo04Z9H/
AgMBAAECggEAEleaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/Hl
\nfvCarftGgMaYWPSONCJRMXB7tPwpQu19esjz4Z/cR2Je4fTLPrffGUsHFgZjv5OQB
\nZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr\nciu9YkInNEHu6uRJ5g/
eGGX3KQynTvIhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M\nEGpfYI6AdHIwFZcT/
```



```
RNAxhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7Ale\nkrguPtFv1vWklg
+bUfHgGaiAEYTpAUN9t2DVliijgQKBgQDnYMMsaF0r557CM1CT
\nXUqgCZ08MKeV2jf2drlxRRwRL33SksQbzAQ/qrLdT7GP3sCGqvKxWY2FPdFYf8kx
\nGcCeZPcleZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/fbwjP7dt
\nJ7n8EzkRUNE6aIMHOFEEych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr
\niWgTWHXPZxUQaYhpjXo6+IMI6DpExiDgBAkMzJGlvS7yQiYWU+wthAr9urbWYdGZ
\nIS6VjoTkF6r7VZoLXX0fbuXh6lm8K8lQRfBpJff56p9phMwaBpDNDrfpHB5utBU\nxs40yldp6wKBgQC69Cp/
xUwTX7GdxQzEJctYiKnBHKcspAg38zJf3bGSXU/jR4eB\n1IVQhELGI9CbKSdzKM71GyElmix/
T7FnSHIWlho1qVo6AQyduNWnAQD15pr8KAd\nXGXAZZ1FQcb3KYa
+2fflERmazdOTwJYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak\n/735uP20KKqhNehZpC2dJei7OilgRhCS/
dKASUXHSW4fptBnUxACYocdDxtY4Vha\nf17FPMdvGL8ioYbvlHFh
+X0Xs9r1S8yeWnHoXMB6eXWmYKMJrAoveLa+2cFm1Agf
\n7nLhA4R4lqm9lpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAjkD4wHW54PwD4Ctfk9o
\njHjWB7pQlUYpTZO9dm+4fpCMn9Okf43AE2yAOaAP94GdzdDjKxfciXKcsYr9lIuk
\nfaoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BUIGKMWXzuEd\n3fy
+1rCUwzOp9LSjtYf4ege\n-----END PRIVATE KEY-----",
"certificate" : "-----BEGIN CERTIFICATE-----
\nMIIC4TCCAcmgAwIBAgICERewDQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXID
\nb21wYU55IENBMBA4XDTE4MDcwMjEzMTU0N1oXDTQ1MTE5NzEzMjU0N1owFDESMBAG
\nA1UEAwWJbG9jYWxob3N0MIIlBlJANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
+DNud1p/
b4XVM6I3rY7+Cfge5GMLDIUxIHXCfCp19Z3807yNpLF5\nU0NqPQZKUrZz3rQeLN9mYiUTJZPutYIFDDbB8CtI
gV+eyU9yYJslWx/Bm5kWNPh9\n7B9Yu9pbp2u6zDA99IC4ekKD93KuzzlnLmSle4Y3dbYwk0LpMDL6lfCHKt/
W7jaS\niAzsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylYKy4zgnv1tn/K
\nny09cxLKAftgoZWQD2FAZJf9F7k1kYNwqlTz3CPLZUUn7yw3nkOOtLMI28IEv0Wy
\nYd7CMJQK51NPJBKNOGfR/wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29t\nhnhwQKUuUvJhwR/
AAABMBMGAA1UdJQQMMAoGCCsGAQUFBwMBMA0GCsGSIb3DQEBCwUA
\nA4IBAQA8lMQJxaTey7EjXtRLSVIEAMftAQPG6jjNQuvIBQYUDauDT4W2XUZ5wAn
\nnjiOyQ83va672K1G9s8n6xlH+xwwdSNnozaKzC87vwSeZKlOdI9I5I98TGKl6OoDa
\nnezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPRLYlp1HMnl6hkjPk4PCZ
\nnwKnh0dlScati9Cct3UzXSNJOSLalKdHErH08lqd+1BchScxCfk0xNITn1HZZGml\n
+vbmunok3A2luc14rnsrbcGyqXGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZ\niYsGDVN+9QBd0eYUHce
+77s96i3l\n-----END CERTIFICATE-----"
}
```

Example Responses

Status code: 201

Successful request.

```
{
  "certificate" : {
    "private_key" : "-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDQVAbOLe5xNf4M253Wn9vhdUzojetjv4J
+B7kYwsMhRcgdcj8KcN1nfzTvl2ksXITQ2o9BkpStnPetB4s32ZiRMIk
+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH172luna7rMMD30gH6QoP3cq7PGWcuZKV7hjd1tjCT
QukwMvqV8lqc39buNplgDOWzEP5AqXtCOFYn6RTH5SRug4hKNN7sT1eYMSlHu7wtEBDKVgrLjOCe/
W2f8rLT1zEsoAW2ChlZAPYUBkl/0XuTWRg3CohPPcl+UtlRSfvlDeeQ460swjbgwS/RbJh3slwICRLU08kEo04Z9H/
AgMBAAECggEAEleaQqHCWZk/HyYN0Am/GJSgFa2tD60SXY2fUieh8/
HlfvCarftGgMaYWPSPNCJRMXB7tPwpQu19esjz4Z/
cR2Je4fTLPrffGUshFGZjv5OOBZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNK
Krciu9YkInNEHu6uRJ5g/eGGX3KQynTvIhnOVGAJvJTXcoU6fm7gYdHAD6jk9lc9MEGpfYI6AdHlwFZcT/
RNAxhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7Ale\nkrguPtFv1vWklg
+bUfHgGaiAEYTpAUN9t2DVliijgQKBgQDnYMMsaF0r557CM1CTXUqgCZ08MKeV2jf2drlxRRwRL33SksQbzAQ/
qrLdT7GP3sCGqvKxWY2FPdFYf8kxGcCeZPcleZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/
fbwjP7dt7n8EzkRUNE6aIMHOFEEych/
PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLrIwGtWHXPZxUQaYhpjXo6+IMI6DpExiDgBAkMzJGlvS7y
QiYWU
+wthAr9urbWYdGZIS6VjoTkF6r7VZoLXX0fbuXh6lm8K8lQRfBpJff56p9phMwaBpDNDrfpHB5utBUxs40yldp6w
KBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zJf3bGSXU/jR4eB\n1IVQhELGI9CbKSdzKM71GyElmix/
T7FnSHIWlho1qVo6AQyduNWnAQD15pr8KAd\nXGXAZZ1FQcb3KYa
+2fflERmazdOTwJYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak/735uP20KKqhNehZpC2dJei7OilgRhCS/
dKASUXHSW4fptBnUxACYocdDxtY4Vhaf17FPMdvGL8ioYbvlHFh+X0Xs9r1S8yeWnHoXMB6eXWmYKMJrAoveLa
+2cFm1Agf7nLhA4R4lqm9lpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAjkD4wHW54PwD4Ctfk9ojHjWB7pQlUYpT
ZO9dm
+4fpCMn9Okf43AE2yAOaAP94GdzdDjKxfciXKcsYr9lIukfaoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO3
8a5gZaOm/BUIGKMWXzuEd3fy+1rCUwzOp9LSjtYf4ege-----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-----
MIIC4TCCAcmgAwIBAgICERewDQYJKoZIhvcNAQELBQAwFzEVMBMGGA1UEAxMMMTXlDb21wYW55IENBMB4X
DTE4MDcwMjEzMjU0N1oXDQ1MTExNzEzMjU0N1owFDESMBAGA1UEAwwJbG9jYWxob3N0MIIlBjANBgkqh
kiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0FQGzi3ucTX+DNud1p/
b4XVM6I3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5U0NqPQZKUrZz3rQeLN9mYiUTJZPutYlFDDbB8CtIgV
+eyU9yYJslWx/Bm5kWNPh97B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/
W7jaSIazlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylyKy4zgnv1tn/
Ky09cxLKAftgoZWQD2FAZJf9F7k1kYNwqlTz3CPILZUUn7yw3nkOOTLMI28IEv0WyYd7CMJQks1NPJBKNOGfR/
wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29thwQKuUvJhwR/
AAABMBMGGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCsGSIb3DQEBCwUAA4IBAQA8IMQJxaTey7EjXtRLSVl
EAMftAQPG6jjjNQvIBQYUDauDT4W2XUZ5wAnjiOyQ83va672K1G9s8n6xlH
+xwwdSNnozaKzC87vwSeZKIOdl9I5I98TGI6OoDaezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPR
LYlp1HMnl6hkjPk4PCZwKnha0dlScati9CCt3UzXSNJOSLalKdHrH08lqd+1BchScxChk0xNITn1HZZGml
+vbmunok3A2luc114rnsrbkGYqXGikySN6B2cRLBDK4Y3wChiW6NVytVqcx5/mZiYsGDVN+9QBd0eYUHce
+77s96i3l-----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 = "{projectId}";

        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-----
MIIC4TCCAcmgAwIBAgICEREWdQYJKoZIhvcNAQELBQAwFzEVMBMGGA1UEAxMMTXID
b21wYW55IENBMB4XDTE4MDcwMjEzMTU0N1oXDTE4MTExNzEzMTU0N1owFDESMBAG
A1UEAwJbG9jYWxob3N0MIIlBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
0FQGzi3ucTX+DNud1p/b4XVM6I3rY7+Cfge5GMLDIUHXHCfCgp19Z3807yNpLF5
U0NqPQZKUrZz3rQeLN9mYiUTJZPutYIFDDbB8CtlgV+eyU9yYJslWx/Bm5kWNPh9
7B9Yu9pbb2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwkOLpMDL6lfCHkt/W7jaS
IAzlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylyKy4zgnv1tn/K
y09cxLKAftgoZWQD2FAZJf9F7k1kYNwqlTz3CPILZUUn7yw3nkOOtLMl28IEv0Wy
Yd7CMJQkS1NPJBKNOGfR/wIDAQABozowODAhBgNVHREEGjAygpkb21haW4uY29t
hwQKUUVhJwR/AAABMBMGGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCsGSIb3DQEBCwUA
A4IBAQA8IMQJxaTey7EjXtRLSVLEAMftAQPG6ijjNQuvIBQYUDauDT4W2XU25wAn
jiOyQ83va672K1G9s8n6xlH+xwwdSNnozaKzC87vwSeZKI0dl9I5I98TKI6OoDa
ezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPRLYlp1Hmnl6hkjPk4PCZ
wKnha0dlScati9Cct3UzXSNJOSLalKdHErH08lqd+1BchScxChk0xNITn1HZZGml
+vbmunok3A2luc14rnsrckbGYqGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZ
iYsGDVN+9QBd0eYUHce+77s96i3l
-----END CERTIFICATE-----")
    .withName("My Certificate")
    .withPrivateKey("-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQQDQVAbOLe5xNf4M
253Wn9vhdUzojetv4J+B7KYwsMhRcgdcJ8KcN1nfzTvl2ksXLTQ2o9BkpStnPe
tB4s32ZiJRMlk+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM
MD30gLh6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8lcq39buNplgDOWZEP5AzqXt
COFYn6RTH5SRug4hKNN7sT1eYMsLHu7wtEBDKVgrLjOCe/W2f8rLT1zEsoAW2Chl
ZAPYUBkl/0XuTWRg3CohPPcl+UtlRSfvLDeeQ460swjbgwS/RbJh3slwlCRLU08k
Eo04Z9H/AgMBAAECCggEAEleaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/Hl
fvCArftGgMaYWPSPNCJRMXB7tPwpQu19esjz4Z/cR2Je4fTLPrffGUsHfGzjv5OQB
ZVe4as5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr
ciu9YklNNEHu6uRJ5g/eGGX3KQynTvVlhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M
EGpfYI6AdHlwFZcT/RNAXhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7Ale
krgruPtFV1vWklg+bUfhgGaiAEYTPAUN9t2DVliijgQKBgQDnYMMsaF0r557CM1CT
XUqgCZ08MKeV2jf2drLxRRwRl33SksQzbAQ/qRLd7GP3sCGqvkvxWY2FPdFYf8kx
GcCeZPcleZYQAM41pjtsaM8tVbLWVR8UtGBuQoPSPH7JNF3Tm/JH/fbwjpiP7dt
J7n8EzkrUNE6alMHOFEEych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr
iWgTWHXPZuXQaYhpiXo6+IMI6DpExiDgBAKMzJGlv57yQiYWU+withAr9urbWYdGZ
lS6VjoTkF6r7VZolLX0fbuXh6lm8K8lQRfBpJff56p9phMwaBpDNDrfpHB5utBU
xs40yldp6wKBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zf3bGSXU/jr4eB
1lVQhELG9CbKSdzKM71GyElmix/T7FnSHIWIho1qVo6AQyduNWnAQD15pr8KAd
XGXAZZ1FQcb3KYa+2fflERMazdOTwYz0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak
/735uP20KKqhNehZpC2dJei7OilgRhCS/dKASUXHSW4fptBnUxACYocdDxtY4Vha
fl7FPMdvGL8ioYbvlHFH+X0Xs9r1S8yeWnHoXMB6eXWmYKMrAoveLa+2cFm1Agf
7nLhA4R4lqm9lpV6SKegDUKR4fxp9pPyodZPqBLLAoGBAJkD4wHW54PwD4Ctfk9o
jHjWB7pQLiYpTZO9dm+4fpCMn9Okf43AE2yAOaAP94GdzdDJkxfciXKcsYr9lIuk
faoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BUIGKMWXzuEd
3fy+1rCUwzOp9LSjtYf4ege
-----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.getStatusCode());
        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-----
MIIC4TCCAcmgAwIBAgICEREdDQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXlD
b21wYW55IENBMB4XDTE4MDcwMjEzMjU0N1oXDTE4MTExNzEzMjU0N1owFDESMBAG
A1UEAwwJbG9jYWxob3N0MIIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
0FQGzi3ucTX+DNud1p/b4XVM6l3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5
U0NqPQZKUrZz3rQeLN9mYiUTJZPutYIFDDbB8CtIgV+eyU9yYJslWx/Bm5kWNPh9
7B9Yu9pbbp2u6zDA99IC4ekkD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/W7jaS
IAZlsxD+QM6l7QjWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQyLYKy4zgnv1tn/K
y09cxLKAftgoZWQD2FAZJf9F7k1kYNwqlTz3CPLZUUn7yw3nkOOtLMI28IEv0Wy
Yd7CMJQkS1NPJBKNOGfR/wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29t
hwQKuUvJhwR/AAABMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAOGCSqGSIb3DQEBCwUA
A4IBAQA8lMQJxaTey7EjXtRLSVIEAMftAQPG6jijNQuvIBQYUDauDT4W2XUZ5wAn
jiOyQ83va672K1G9s8n6xlH+xwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDa
ezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPRLYlp1HMnl6hkjPk4PCZ
wKnha0dlScatI9Cct3UzXSNJOSLalKdHERH08lqd+1BchScxCfk0xNITn1HZZGml
+vbmunok3A2luc14rnsrbkGyqGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZ
iYsGDVN+9QBd0eYUHce+77s96i3l
-----END CERTIFICATE-----",
            name="My Certificate",
            private_key="-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDQVAbOLe5xNf4M
253Wn9vhdUzojetjv4J+B7kYwsMhRcgdcJ8KCnX1nfzTvI2ksXLTQ2o9BkpStnPe
tB4s32ZiJRMlk+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM
MD30gH6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8lcq39buNplgDOWzEP5AzqXt
COFYn6RTH5SRug4hKNN7sT1eYMsIHu7wtEBDKVgrLjOCe/W2f8rLT1zEsoAW2Chl
ZAPYUBkl/0XuTWRg3CohPPcl+UtlRSfvlDeeQ460swjbgwS/RbJh3slwlCRLU08k
Eo04Z9H/AgMBAAECggEAEleaQqHCWZk/HyYN0Am/GJSFfa2tD60SXY2fUieh8/Hl
fvCArftGgMaYWPNSNCJRMXB7tPwpQu19esjz4Z/cR2J4fTLPrffGUsHFgZjv5OQB
-----END PRIVATE KEY-----"
        )
        request.set_certificatebody(certificatebody)

        response = client.create_certificate(request)
        print(response.to_dict())
    except exceptions.ApiException as e:
        print("The api has error: %s" % e)
```

```
ZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr
ciu9YklnNEHu6uRJ5g/eGGX3KQynTvVlhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M
EGpfYI6AdHlwFZcT/RNAXhP82lg2gUJSgAu66FFdJmWqXKbafKdP3zq4Up8a7Ale
krquPtfV1vWklg+bUFhgGaiAEYTpAUN9t2DVliijgQKBgQDnYMMsaF0r557CM1CT
XUqgCZo8MKeV2jf2drlxRRwRL33SksQbzAQ/qrLdT7GP3sCGqvkvxWY2FPdFYf8kx
GcCeZPcleZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/fbwjP7dt
J7n8EzkRUNE6aIMHOFEEych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr
iWgTWHXPZxUQaYhpjXo6+lMI6DpExiDgBAkMzJGlvS7yQiYWU+wthAr9urbWYdGZ
IS6VjoTkF6r7VZoILXX0fbuXh6lm8K8lQRfBpJff56p9phMwaBpDNDrfpHB5utBU
xs40Yldp6wKBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zf3bGSXU/jR4eB
1lVQhELGI9CbKSdzKM71GyElmix/T7FnJSHIWlho1qVo6AQyduNWnAQD15pr8KAd
XGXAZZ1FQcb3KYa+2fflERmazdOTWjYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak
/735uP20KKqhNehZpC2dJei7OilgRhCS/dKASUXHSW4fptBnUxACYocdDxtY4Vha
fl7FPMdvGl8ioYbvlHFh+X0Xs9r1S8yeWnHoXMB6eXWmYKMrAoveLa+2cFm1Agf
7nLhA4R4lqm9lpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAJkD4wHW54Pw4Ctfk9o
jHjWB7pQlUYpTZO9dm+4fpCMn9Okf43AE2yAOaAP94GdzdDJkxfciXKcsYr9lIuk
faoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BUlGKMWXzuEd
3fy+1rCUwzOp9LSjtUYf4ege
-----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-----  
MIIC4TCCAcmgAwIBAgICERewDQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXID  
b21wYW55IENBMB4XDTE4MDcwMjEzMjU0N1oXDTQ1MTExNzEzMjU0N1owFDESMBAG  
A1UEAwwjbG9jYWxob3N0MIIlBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA  
0FQGzi3ucTX+DNud1p/b4XVM6l3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5  
U0NqPQZKURZz3rQeLN9mYiUTJZPutYIFDDbB8CtlgV+eyU9yYslWx/Bm5kWNPh9  
7B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/W7jaS  
lAzlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQyLYKy4zgnv1tn/K  
y09cxLKAftgoZWQD2FAZJf9F7k1kYNwqITz3CPILZUUn7yw3nkOOTLMI28IEv0Wy  
Yd7CMJQkS1NPJBKNOGfR/wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29t  
hwQKUUVjhwR/AAABMBMGA1UdJQQMMAoGCCSGAQUFBwMBMA0GCsGSIb3DQEBCwUA  
A4IBAQA8lMQJxaTey7EjXtRLSVIEAMftAQPG6jijNQvIBQYUDauDT4W2XU5wAn  
jiOyQ83va672K1G9s8n6xlH+xwwdSNnozaKzC87vwSeZKI0dl9I5198TGKI6OoDa  
ezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPRLYLzp1HMnl6hkpK4PCZ  
wKnha0dlScat9CCt3UzXSJOSLalKdHERH08lqd+1BchScxChk0xNITn1HZZGml  
+vbmunok3A2luc14rnsrckbGyqGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZ  
iYsGDVN+9QBd0eYUHce+77s96i3l  
-----END CERTIFICATE-----"  
    nameCertificate:= "My Certificate"  
    privateKeyCertificate:= "-----BEGIN PRIVATE KEY-----  
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDQVAbOLe5xNf4M  
253Wn9vhdUzojetjv4J+B7kYwsMhRcgdcJ8KcnX1nfzTvi2ksXITQ2o9BkpStnPe  
tB4s32ZiJRMlk+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM  
MD30gLvH6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8lcq39buNplgDOWzEP5AzqXt  
COFYn6RTH5SRug4hKNN7sT1eYMSlHu7wtEBDKVgrLjOCe/W2f8rL1zEsoAW2Chl  
ZAPYUBkl/0XuTWRg3CohPPcl+UtlRSfvLDeeQ460swjbgwS/RbJh3slwCRLU08k  
Eo04Z9H/AgMBAAECggEAEleaQqHCWZk/HyYN0Am/GJSgFa2tD60SXY2fUieh8/Hl  
fvCArftGgMaYWPNSCJRMXB7tPwpQu19esjz4Z/cR2Je4fTLPrffGUsHFGzjv5OQB  
ZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr  
ciu9YklNNEHu6uRJ5g/eGGX3KQynTvVlhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M  
EGpfYI6AdHlwFZcT/RNAXhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7Ale  
rguPtFv1vWklg+bUFhgGaiAEYTPAUN9t2DVliijgQKBgQDnYMMsaF0r557CM1CT  
XUqgCZo8MKeV2jf2drLxRRwRL33SksQbzAQ/qRLd7GP3sCGqvkxWY2FPdFYf8kx  
GcCeZPcleZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/fbwjpp7dt  
J7n8EzkRUNE6alMHOFEEych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr  
iWgTWHXPZxUQaYhpjXo6+IMI6DpExiDgBAKmZJGlvS7yQiyWU+wthAr9urbWYdGZ  
IS6VjoTkf6r7VZoLXX0fbuXh6lm8K8lQRfBpJff56p9phMwaBpDNDrfpHB5utBU  
xs40yldp6wKBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zlf3bGSXU/jR4eB  
1lVQhELGI9CbKSdzKM71GyElmix/T7FnJSHIwlho1qVo6AQyduNWnAQD15prKAd  
XGXAzz1FQcb3KYa+2ffIERmazdOTwjYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak  
/735uP20KqkNehZpC2dJei7OilgRhCS/dKASUXHSW4fptBnUxACYocdDxtY4Vha  
fl7FPMdvG8l0YbvlHFh+X0Xs9r1S8yeWnHoXMB6eXWmYKMrAoveLa+2cFm1Agf  
7nLhA4R4lqm9lpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAJkD4wHW54PwD4Ctfk9o  
jHjWB7pQlUYpTZO9dm+4fpCMn9Okf43AE2yAOaAP94GdzdDjKxfciXKcsYr9IluK  
faoXgjkR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BULGKMWXzuEd  
3fy+1rCUwzOp9LSjtYf4ege  
-----END PRIVATE KEY-----"  
    typeCertificate:= model.CreateCertificateOptionTypeEnum().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	Successful request.

Error Codes

See [Error Codes](#).

5.7.2 Querying Certificates

Function

This API is used to query the certificates used by the load balancer.

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 5-197 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Table 5-198 Query Parameters

Parameter	Mandatory	Type	Description
marker	No	String	Definition: Specifies the ID of the last record on the previous page. Constraints: • This parameter must be used together with limit. • If the parameter is not specified, only resources on the first page are queried. • This parameter cannot be left blank or set to an invalid ID. Range: N/A Default value: N/A
limit	No	Integer	Definition: Specifies the number of records returned on each page. Constraints: N/A Range: 0 to 2000 Default value: 2000

Parameter	Mandatory	Type	Description
page_reverse	No	Boolean	Definition: Specifies whether to use reverse query. Constraints: • This parameter must be used together with limit. • If page_reverse is set to true and you want to query the resources on the previous page, set the value of marker to the value of previous_marker. Range: • true: Query resources on the previous page. • false: Query resources on the next page. Default value: false
id	No	Array of strings	Definition: Specifies the certificate ID. Multiple IDs can be used for query in the format of <i>id=xxx&id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
name	No	Array of strings	Definition: Specifies the certificate name. Multiple names can be used for query in the format of <i>name=xxx&name=xxx</i> . Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
description	No	Array of strings	Definition: Provides supplementary information about the certificate. Multiple descriptions can be used for query in the format of <i>description=xxx&description=xx</i> . Constraints: N/A Range: N/A Default value: N/A
admin_state_up	No	Boolean	Definition: Specifies the administrative status of the certificate. Constraints: N/A Range: • true: The certificate is available. • false: The certificate is unavailable. Default value: N/A
domain	No	Array of strings	Definition: Specifies the domain names used by the server certificate. Multiple domain names can be used for query in the format of <i>domain=xxx&domain=xxx</i> . Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
type	No	Array of strings	Definition: Specifies the certificate type. Multiple types can be used for query in the format of <i>type=xxx&type=xxx</i> . Constraints: N/A Range: • server: server certificates • client CA certificates • server_sm: server SM certificates Default value: N/A
scm_certificate_id	No	Array of strings	Definition: Specifies the ID of the certificate managed on Cloud Certificate Manager (CCM). Multiple IDs can be used for query in the format of <i>scm_certificate_id=xxx&scm_certificate_id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
common_name	No	Array of strings	Definition: Specifies the primary domain name of the certificate. Multiple domain names can be used for query in the format of <i>common_name=xxx&common_name=xxx</i> . Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
fingerprint	No	Array of strings	Definition: Specifies the fingerprint of the certificate. Multiple fingerprints can be used for query in the format of <i>fingerprint=xxx&fingerprint=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
source	No	Array of strings	Definition: Specifies the source of the certificate. Multiple sources can be used for query in the format of <i>source=xxx&source=xxx</i> . Constraints: N/A Range: ● scm: certificates from CCM ● Empty: self-signed certificates Default value: N/A
protection_status	No	Array of strings	Definition: Specifies the protection status. Multiple statuses can be used for query in the format of <i>protection_status=xxx&protection_status=xxx</i> . Constraints: N/A Range: ● nonProtection: The resource is not protected. ● consoleProtection: Modification is not allowed on the console. Default value: N/A

Parameter	Mandatory	Type	Description
protection_reason	No	Array of strings	Definition: Specifies why modification protection is enabled. Multiple values can be used for query in the format of <i>protection_reason=xxx&protection_reason=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
enterprise_project_id	No	Array of strings	Definition: Specifies the ID of the enterprise project. Multiple values can be used for query in the format of: <i>enterprise_project_id=xxx&enterprise_project_id=xxx</i> . Constraints: • If enterprise_project_id is not specified, resources in all enterprise projects are queried by default. Fine-grained authorization is performed. The elb:certificates: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:certificates:list permission are queried. Range: N/A Default value: N/A

Request Parameters

Table 5-199 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200**Table 5-200** Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
page_info	PageInfo object	Definition: Specifies the pagination information.
certificates	Array of CertificateInfo objects	Definition: Lists the certificates.

Table 5-201 PageInfo

Parameter	Type	Description
previous_marker	String	Definition: Specifies the ID of the first record in the pagination query result. If page_reverse is set to true , this parameter is used together to query resources on the previous page. Range: N/A

Parameter	Type	Description
next_marker	String	Definition: Specifies the ID of the last record in the pagination query result. It is usually used to query resources on the next page. Range: N/A
current_count	Integer	Definition: Specifies the number of records returned on the current page. Range: N/A

Table 5-202 CertificateInfo

Parameter	Type	Description
admin_state_up	Boolean	Definition: Specifies the administrative status of the certificate. This parameter does not take effect whether it is set to true or false . Range: • true: The certificate is available. • false: The certificate is unavailable.
certificate	String	Definition: Specifies the certificate content. It supports certificate chains with a maximum of 11 layers (including certificates and certificate chains). Range: The value must be PEM encoded, and can contain a maximum of 65,536 characters.
description	String	Definition: Provides supplementary information about the certificate. Range: 0 to 255 characters.

Parameter	Type	Description
domain	String	Definition: Specifies the domain names used by the server certificate. Range: 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	Definition: Specifies the certificate ID. Range: The value consists of 32 digits and lowercase letters.
name	String	Definition: Specifies the certificate name. Range: 0 to 255 characters.
private_key	String	Definition: Specifies the private key of the server certificate. Range: The value must be PEM encoded, and can contain a maximum of 8,192 characters.
type	String	Definition: Specifies the certificate type. Range: • server: server certificates • client CA certificates • server_sm: server SM certificates
created_at	String	Definition: Specifies the creation time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.

Parameter	Type	Description
updated_at	String	Definition: Specifies the update time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.
expire_time	String	Definition: Specifies the time when the certificate expires. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.
project_id	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Range: The value can contain a maximum of 32 characters, including digits and lowercase letters.
enc_certificate	String	Definition: Specifies the content of the server SM certificate. It supports certificate chains with a maximum of 11 layers (including certificates and certificate chains). Range: The value must be PEM encoded, and can contain a maximum of 65536 characters.
enc_private_key	String	Definition: Specifies the private key of the server SM certificate. Range: The value must be PEM encoded, and can contain a maximum of 8,192 characters.
scm_certificate_id	String	Definition: Specifies the ID of the certificate managed on Cloud Certificate Manager (CCM). Range: N/A
common_name	String	Definition: Specifies the primary domain name of the certificate. Range: N/A
fingerprint	String	Definition: Specifies the fingerprint of the certificate. Range: N/A
subject_alternative_names	Array of strings	Definition: Specifies all the domain names of the certificate. Range: N/A

Parameter	Type	Description
source	String	Definition: Specifies the source of the certificate. Range: • scm: certificates from CCM • Empty: self-signed certificates
protection_status	String	Definition: Specifies the protection status. Range: • nonProtection: The resource is not protected. • consoleProtection: Modification is not allowed on the console.
protection_reason	String	Definition: Specifies why modification protection is enabled. Range: N/A

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_certificate",
    "type": "server",
    "domain": null,
    "description": "description for certificatehhhh",
    "private_key": "-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBAKggwggSkAgEAAoIBAQDQVAbOLe5xNf4M253Wn9vhdUzojetjv4J
+B7kYwsMhRcgdcJ8KcX1nfzTvl2ksXITQ2o9BkpStnPetB4s32ZiJRMlk
+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rMMD30gLh6QoP3cq7PGWcuZKV7hjd1tjCT
QukwMvqV8lcq39buNplgDOWzEP5AzqXtCOFYn6RTH5SRug4hKNN7sT1eYMSlHu7wtEBDKVgrLjOCe/
W2f8rLT1zEsoAW2ChlZAPYUBkl/0XuTWRg3CohPPcl+UtlRSfvLDeeQ460swjbgwS/RbJh3slwlCRLU08kEo04Z9H/
AgMBAAECggEAEleaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/
HlfvCARftGgMaYWPNSCJRMXB7tPwpQu19esjz4Z/
cR2Je4fTLPrffGUshFgZjv5OQBVZe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNK
Krciu9YkInNEHu6uRJ5g/eGGX3KQynTvVlhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9MEGpfYI6AdHlwFZcT/
RNAxhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7AlekguPtFv1vWklg
+bUfhGaiAEYTPAUN9t2DVliijgQKBgQDnYMMsaF0r557CM1CTXUqgCZo8MKeV2jf2drLxRRwRL33SksQbzAQ/
qrLdT7GP3sCGqvKxWY2FPdFYf8kxGcCeZPcleZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/
fbwjPjP7dtU7n8EzkRUNE6aIMHOFEEych/
PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLriWgTWHXPZxUqaYhpjXo6+IMI6DpExiDgBAkMzJGlvS7y
QiyWU
+wthAr9urbWYdGZIS6VjoTkF6r7VZolLXX0fbuXh6lm8K8lQRfBpJff56p9phMwaBpDNDrfpHB5utBUxs40Yldp6w
```

```
KBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zJf3bGSXU/jR4eB1lVQhELGI9CbKSdzKM71GyElmix/
T7FnJSHIWlho1qVo6AQyduNwNAQD15pr8KAdXGXAZZ1FQcb3KYa
+2fflERmazdOTwJYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak/735uP20KKqhNehZpC2dJei7OilgRhCS/
dKASUXHSW4fptBnUxACYocdDxtY4Vhafi7FPMdvGL8ioYbvlHFh+X0Xs9r1S8yeWnHoXMB6eXWmYKMrAoveLa
+2cFm1Agf7nLhA4R4lqm9lpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAJkD4wHW54PwD4Ctfk9ojHjWB7pQLUYpT
ZO9dm
+4fpCMn9Okf43AE2yAOaAP94GdzdDjKxfciXKcsYr9lIukfaoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO3
8a5gZaOm/BULGKMWXzuEd3fy+1rCUwzOp9LSjtYf4ege-----END PRIVATE KEY-----",
  "certificate" : "-----BEGIN CERTIFICATE-----
MIIC4TCCAcmgAwIBAgICEREWdQYJKoZIhvcNAQELBQAwFzEVMBMGGA1UEAxMMTXlDb21wYW55IENBMB4X
DTE4MDcwMjEzMjU0N1oXDTQ1MTE5NzEzMjU0N1owFDESMBAGA1UEAwwJbG9jYWxob3N0MIIlBjANBgkqh
kiG9wOBAQEFAAOCAQ8AMIIBBgKCAQEA0FQGi3ucTX+DNud1p/
b4XVM6l3rY7+Cfge5GMLDIUIHXCFcGp19Z3807yNpLF5U0NqPQZKUrZz3rQeLN9mYiUTJZPutYIFDDbB8CtIgV
+eyU9yYJslWx/Bm5kWNPh97B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/
W7jaSlAzlsx+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQyLYKy4zgnv1tn/
Ky09cxLKAftgoZWQD2FAZJf9F7k1kYNwqlTz3CPILZUUn7yw3nkOOtLMI28IEv0WyYd7CMJQks1NPJBKNOGfR/
wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29thwQKuUvJhwR/
AAABMBMGGA1UdJQQMMAoGCCSGAQUFBwMBMA0GCsGQSIb3DQEBCwUAA4IBAQA8IMQJxaTey7EjXtRLSVL
EAMftAQPG6jjjNQvIBQYUDauDT4W2XUZ5wAnjiOyQ83va672K1G9s8n6xlH
+xmwdSNnozaKc87vwSeZKIOdl9i5I98TGKI6OoDaezmzCwQYtHBMVQ4c7ML8554Ft1mWSt4dMAK2rzNYjvPR
LYlp1HMnl6hkjPk4PCZwKnha0dlScati9Cct3UzXSNJOSLalKdHErH08lqd+1BchScxCfk0xNITn1HZZGml
+vbmunok3A2luc14rnsrckbGYqXGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZiYsGDVN+9QBd0eYUHe
+77s96i3l-----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-----
MIIEvgIBADANBgkqhkiG9wOBAQEFAASCBKgwggSkAgEAAoIBAQDQVAbOLe5xNf4M253Wn9vhdUzojetjv4J
+B7kYwsMhRcgdcJ8KcN1nfzTvl2ksXITQ2o9BkpStnPetB4s32ZiJRMlk
+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rMMD30gH6QoP3cq7PGWcuZKV7hjd1tjCT
QukwMvqV8lCq39bunPlgDOWzEP5AzaqXtCOFYn6RTH5SRug4hKNN7sT1eYMstHu7wtEBDKVgrLjOCe/
W2f8rLT1zEsoAW2ChIZAPYUBkl/0XuTWRg3CohPPcl+UtlRSfvlDeeQ460swjbgwS/RbJh3slwCRLU08kEo04Z9H/
AgMBAAECggEAEleaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/
HlfvCARftGgMaYWPSNCRJRMXB7tPwpQu19esjz4Z/
cR2Je4fTLPrffGUsHFgZjv5OQBZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNK
Krciu9YklnNEHu6uRj5g/eGGX3KQynTv/IhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9MEGpfYl6AdHlwFZcT/
RNAxhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7AlekguPtfV1vWklg
+buFhgGaiAEYTpAUN9t2DVliijgQKBgQDnYMMsaF0r557CM1CTXUqgCZ08MKeV2jf2drLxRRwRL33SksQbzAQ/
qrLdT7GP3sCGqvKxWY2FPdFYf8kxGcCeZPcleZYQCAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/
fbwjPjP7dtJn8EzkRUNE6aIMHOFEEych/
PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLriWgTWHXPZxUQaYhpjXo6+IMI6DpExiDgBAkMzJGlvS7y
QiYwU
+wthAr9urbWYdGZLS6VjoTkF6r7VZoLXX0fBuXh6l8m8K8lQRfBpJff56p9phMwaBpDNDrfpHB5utBUxs40yldp6w
KBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zJf3bGSXU/jR4eB1lVQhELGI9CbKSdzKM71GyElmix/
T7FnJSHIWlho1qVo6AQyduNwNAQD15pr8KAdXGXAZZ1FQcb3KYa
+2fflERmazdOTwJYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak/735uP20KKqhNehZpC2dJei7OilgRhCS/
dKASUXHSW4fptBnUxACYocdDxtY4Vhafi7FPMdvGL8ioYbvlHFh+X0Xs9r1S8yeWnHoXMB6eXWmYKMrAoveLa
+2cFm1Agf7nLhA4R4lqm9lpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAJkD4wHW54PwD4Ctfk9ojHjWB7pQLUYpT
ZO9dm
+4fpCMn9Okf43AE2yAOaAP94GdzdDjKxfciXKcsYr9lIukfaoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO3
8a5gZaOm/BULGKMWXzuEd3fy+1rCUwzOp9LSjtYf4ege-----END PRIVATE KEY-----",
  "certificate" : "-----BEGIN CERTIFICATE-----
MIIC4TCCAcmgAwIBAgICEREWdQYJKoZIhvcNAQELBQAwFzEVMBMGGA1UEAxMMTXlDb21wYW55IENBMB4X
DTE4MDcwMjEzMjU0N1oXDTQ1MTE5NzEzMjU0N1owFDESMBAGA1UEAwwJbG9jYWxob3N0MIIlBjANBgkqh
kiG9wOBAQEFAAOCAQ8AMIIBBgKCAQEA0FQGi3ucTX+DNud1p/
b4XVM6l3rY7+Cfge5GMLDIUIHXCFcGp19Z3807yNpLF5U0NqPQZKUrZz3rQeLN9mYiUTJZPutYIFDDbB8CtIgV
+eyU9yYJslWx/Bm5kWNPh97B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/
W7jaSlAzlsx+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQyLYKy4zgnv1tn/
```

```
Ky09cxLKAftgoZWQD2FAZJf9F7k1kYNwqITz3CPILZUUn7yw3nkOotLMI28IEv0WyYd7CMJQkS1NPJBKNOGfR/
wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29thwQKuUvJhwR/
AAABMBMGGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCsGqSib3DQEBcWUAA4IBAQA8IMQJxaTey7EjXtRLSVL
EAMftAQPG6jijNQvIBQYUDauDT4W2XUZ5wAnjiOyQ83va672K1G9s8n6xlH
+xxwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDaezmzCwQYtHBMVQ4c7ML8554Ft1mWSt4dMAK2rzNYjvPR
LYlp1HmNl6hkjPk4PCZwKnha0dlScati9Cct3UzXSNJOSLaKdHErH08lqd+1BchScxCfk0xNITn1HZZGml
+vbmunok3A2luc14rnsrbcGyqGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZiYsGDVN+9QBd0eYUHce
+77s96i3l-----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
+B7kYwsMhRcgdcJ8KCnX1nfzTvl2ksXITQ2o9BkpStnPetB4s32ZiJRMlk
+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rMMD30gH6QoP3cq7PGWcuZKV7hjd1tjCT
QukwMvqV8lqc39buNplgDOWzEP5AzqXtCOFYn6RTH5SRug4hKNN7sT1eYMstHu7wtEBDKVgrLjOCe/
W2f8rLT1zEsoAW2ChIZAPYUBkl/0XuTWRg3CohPPcl+UtlRSfvLDeeQ460swjbgwS/RbJh3slwCRLU08kEo04Z9H/
AgMBAAECggEAEleaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/
HlfvCarftGgMaYWPSNCRMXB7tPwpQu19esjz4Z/
cR2Je4fTLPrffGUsHFgZjv5OQBZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNK
Krciu9YkInNEHu6uRj5g/eGGX3KQynTvVlhnOVGAJvJTXcoU6fm7gYdHAD6jk9c9MEGpfYl6AdHlWfZcT/
RNAxhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7AlekrquPtfV1vWklg
+buFhgGaiAEYTpAUN9t2DVliijgQKBgQDnYMMsaF0r557CM1CTXUqgCZo8MKeV2jf2drLxRRwRL33KsQbzAQ/
qrLdT7GP3sCGqvkxWY2FPdFYf8kxGcCeZPcleZYQCAM41pjtsaM8tVbLWVVR8UtGBuQoPSph7JNF3Tm/JH/
fbwjpp7dtJ7n8EzkRUNE6aIMHOFEEych/
PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLriWgTWHXPZxUQaYhpjXo6+IMI6DpExiDgBAkMzJGlvS7y
QiYwU
+wthAr9urbWYdGZIS6VjoTkF6r7VZoLXX0fbuXh6lm8K8lQRfBpJff56p9phMwaBpDNDrfpHB5utBUxs40yldp6w
KBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zJf3bGSXU/jR4eB1lVQhELGI9CbKSdzKM71GyElmix/
T7FnJSHIWhlo1qVo6AQyduNwNAQD15pr8KAdXGXAzz1FQcb3KYa
+2fFlERmazdOTwJyZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak/735uP20KKqhNehZpC2dJei7OilRhCS/
dKASUXHSW4fptBnUxACYocdDxtY4Vhafi7FPMdvG8ioYbvlHFH+X0Xs9r1S8yeWnHoXmb6eXWmYKMIrAoVeLa
+2cFm1Agf7nLhA4R4lqm9lpV6SKegDUkR4fxp9pPyodZPqLLaOGBAJkD4wHw54PwD4Ctcfk9ojHjWB7pQLUYpT
ZO9dm
+4fpCMn9Okf43AE2yAOaAP94GdzdDJKxfciXKcsYr9lIukfaoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO3
8a5gZaOm/BUlGKMWXzuEd3fy+1rCUwzOp9LSjtYf4ege-----END PRIVATE KEY-----",
  "certificate" : "-----BEGIN CERTIFICATE-----
MIIC4TCCAcmgAwIBAgICEREwDQYJKoZIhvcNAQELBQAwFzEVMBMGGA1UEAxMNTXlDb21wYy55IENBMB4X
DTE4MDcwMjEzMTU0N1oXDTE4MDcwMjEzMTU0N1owFDESMBAGA1UEAwwJbG9jYXVob3N0M0IIBIjANBgkqh
kiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0FQZi3ucTX+DNud1p/
b4XVM6I3rY7+Cfge5GMLDIUHXfCgP19Z3807yNpLF5U0NqPQZKUrz3rQeLn9mYiUTJZPutYlFDDbB8CtIgV
+eyU9yJslWx/Bm5kWNPh97B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/
W7jaSiAzlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylyKy4zgnv1tn/
Ky09cxLKAftgoZWQD2FAZJf9F7k1kYNwqITz3CPILZUUn7yw3nkOotLMI28IEv0WyYd7CMJQkS1NPJBKNOGfR/
wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29thwQKuUvJhwR/
AAABMBMGGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCsGqSib3DQEBcWUAA4IBAQA8IMQJxaTey7EjXtRLSVL
EAMftAQPG6jijNQvIBQYUDauDT4W2XUZ5wAnjiOyQ83va672K1G9s8n6xlH
+xxwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDaezmzCwQYtHBMVQ4c7ML8554Ft1mWSt4dMAK2rzNYjvPR
LYlp1HmNl6hkjPk4PCZwKnha0dlScati9Cct3UzXSNJOSLaKdHErH08lqd+1BchScxCfk0xNITn1HZZGml
+vbmunok3A2luc14rnsrbcGyqGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZiYsGDVN+9QBd0eYUHce
+77s96i3l-----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.getStatusCode());  
            System.out.println(e.getRequestId());  
            System.out.println(e.getErrorCode());  
            System.out.println(e.getErrorMsg());  
        }  
    }  
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from 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 a certificate used by the load balancer.

Calling Method

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

URI

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

Table 5-203 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
certificate_id	Yes	String	Specifies a certificate ID.

Request Parameters

Table 5-204 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-205 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
certificate	CertificateInfo object	Definition: Specifies the certificate.

Table 5-206 CertificateInfo

Parameter	Type	Description
admin_state_up	Boolean	Definition: Specifies the administrative status of the certificate. This parameter does not take effect whether it is set to true or false . Range: • true: The certificate is available. • false: The certificate is unavailable.
certificate	String	Definition: Specifies the certificate content. It supports certificate chains with a maximum of 11 layers (including certificates and certificate chains). Range: The value must be PEM encoded, and can contain a maximum of 65,536 characters.
description	String	Definition: Provides supplementary information about the certificate. Range: 0 to 255 characters.
domain	String	Definition: Specifies the domain names used by the server certificate. Range: 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	Definition: Specifies the certificate ID. Range: The value consists of 32 digits and lowercase letters.

Parameter	Type	Description
name	String	Definition: Specifies the certificate name. Range: 0 to 255 characters.
private_key	String	Definition: Specifies the private key of the server certificate. Range: The value must be PEM encoded, and can contain a maximum of 8,192 characters.
type	String	Definition: Specifies the certificate type. Range: • server: server certificates • client CA certificates • server_sm: server SM certificates
created_at	String	Definition: Specifies the creation time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.
updated_at	String	Definition: Specifies the update time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.
expire_time	String	Definition: Specifies the time when the certificate expires. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.
project_id	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Range: The value can contain a maximum of 32 characters, including digits and lowercase letters.
enc_certificate	String	Definition: Specifies the content of the server SM certificate. It supports certificate chains with a maximum of 11 layers (including certificates and certificate chains). Range: The value must be PEM encoded, and can contain a maximum of 65536 characters.

Parameter	Type	Description
enc_private_key	String	Definition: Specifies the private key of the server SM certificate. Range: The value must be PEM encoded, and can contain a maximum of 8,192 characters.
scm_certificate_id	String	Definition: Specifies the ID of the certificate managed on Cloud Certificate Manager (CCM). Range: N/A
common_name	String	Definition: Specifies the primary domain name of the certificate. Range: N/A
fingerprint	String	Definition: Specifies the fingerprint of the certificate. Range: N/A
subject_alternative_names	Array of strings	Definition: Specifies all the domain names of the certificate. Range: N/A
source	String	Definition: Specifies the source of the certificate. Range: • scm: certificates from CCM • Empty: self-signed certificates
protection_status	String	Definition: Specifies the protection status. Range: • nonProtection: The resource is not protected. • consoleProtection: Modification is not allowed on the console.
protection_reason	String	Definition: Specifies why modification protection is enabled. Range: N/A

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
+B7kYwsMhRcgdcJ8KCnX1nfzTvl2ksXITQ2o9BkpStnP4B4s32ZiJRMlk
+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rMMD30gH6QoP3cq7PGWcuZKV7hjd1tjCT
QukwMvqV8lq39buNplgDOWzEP5AzqXtCOFYn6RTH5SRug4hKNN7sT1eYMsIHu7wtEBDKVgrLjOCe/
W2f8rLT1zEsoAW2ChZAPYUBkl/OXuTWRg3CohPPcl+UtlRSfvlDeeQ460swjbgwS/RbJh3slwICRLU08Eo04Z9H/
AgMBAEECggEAEleaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/
HlfvCArftGgMaYWP5NJCJRMXB7tPwpQu19esjz4Z/
cR2Je4FTLPrffGUshFgZjv5OQ8BZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8ISETq8YaXngBO6vES9LMhHkNK
Krciu9YklnNEHu6uRJ5g/eGGX3KQynTvVlhnOVGAJvjTxcU6fm7gYdHAD6jk9lc9MEGpfYI6AdHlwFZcT/
RNAxhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7AlekrguPtFv1vWklg
+bUfhGaiAEYTpAUN9t2DVliigQKBgQDnYMMsaF0r557CM1CTXUqgCZo8MKeV2jf2drLxRRwRL33SksQbzAQ/
qrLdT7GP3sCGqvkxWY2FPdFYf8kxGcCeZPcleZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/
fbwjpjP7dtJn8EzkRUNE6aIMHOFeych/
PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYk4aLriWgTWHXPZxUQaYhpjXo6+IMI6DpExiDgBAkMzJGlvS7y
QiYwU
+wthAr9urbWYdGZIS6VjoTkF6r7VZolLXX0fbuXh6lm8K8lQRfBpJff56p9phMwaBpDNDrfpHB5utBUxs40yldp6w
KBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zf3bGSXU/jR4eB1lVQhELGI9CbK5sdzKM71GyElmix/
T7FnJSHIWIho1qVo6AQyduNWnAQD15pr8KAdXGXAZZ1FQcb3KYa
+2fflERmazdOTWjYz0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak/735uP20KKqhNehZpC2dJei7OilRhCS/
dKASUXHSW4fptBnUxACYocdDxtY4Vhaf17FPMdvGl8ioYbvlHFh+XOXs9r1S8yeWnHoXMB6eXWmYKMrAoveLa
+2cFm1Agf7nLhA4R4lqm9lpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAJkD4wHW54PwD4Ctfk9ojHjWB7pQlUYpT
ZO9dm
+4fpCMn9Okf43AE2yAOaAP94GdzdJkxfciXKcsYr9lIukfaoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO3
8a5gZaOm/BULGKMWXzuEd3fy+1rCUwzOp9LSjtUYf4ege-----END PRIVATE KEY-----",
    "certificate" : "-----BEGIN CERTIFICATE-----
MIIC4TCCAcmgAwIBAgICERewDQYJKoZIhvcNAQELBQAwFzEVMBMGGA1UEAxMMTXlDb21wYW55IENBMB4X
DTE4MDcwMjEzMDU0N1oXDTQ1MTExNzEzMjU0N1owFDESMBAGA1UEAwwJbG9jYXVob3N0MIIIBjANBgkqh
kiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAFQgzi3ucTX+DNud1p/
b4XVM6l3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5U0NqPQZKUrZz3rQeLn9mYiUTJZPutYIFDDbB8CtIgV
+eyU9yYslWx/Bm5kWNPh97B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/
W7jaSIAzlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylyKy4zgnv1tn/
Ky09cxLKAftgoZWQD2FAZJf9F7k1kYNwqlTz3CPLZUUn7yw3nkOOTLMI28IEv0WYyYd7CMJQks1NPJBKNOGfR/
wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29thwQKuUvJhwr/
AAABMBMGGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCsGSIb3DQEBCwUAA4IBAQA8IMQJxaTey7EjXtRSLVl
EAMftAQPG6jijNQuvIBQYUDauDT4W2XUZ5wAnjiOyQ83va672K1G9s8n6xtH
+xwwdSNnozaKzC87vwSeZKlOdL9I5I98TGKI6OoDaezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPR
LYlzp1HMnl6hkjPk4PCZwKnha0dScati9CCT3UzXSNJOSLalKdHERH08lqd+1BchScxCfk0xNITn1HZZGml
+vbmunok3A2luc14rnsrckbGYqxGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZiYsGDVN+9QBd0eYUHce
+77s96i3l-----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"
}
```

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 ShowCertificateSolution {

    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();
        ShowCertificateRequest request = new ShowCertificateRequest();
        request.withCertificateId("{certificate_id}");
        try {
            ShowCertificateResponse response = client.showCertificate(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from 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 = ShowCertificateRequest()
    request.certificate_id = "{certificate_id}"
    response = client.show_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.ShowCertificateRequest{}
    request.CertificateId = "{certificate_id}"
    response, err := client.ShowCertificate(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](#).

5.7.4 Updating a Certificate

Function

This API is used to update a certificate used by the load balancer. You can update the certificate content and private key, but not the certificate type.

Note: Updating a certificate will affect the associated listeners.

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 5-207 Path Parameters

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

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-208 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-209 Request body parameters

Parameter	Mandatory	Type	Description
certificate	Yes	UpdateCertificateOption object	Definition: Specifies the parameters for updating a certificate. Constraints: N/A

Table 5-210 UpdateCertificateOption

Parameter	Mandatory	Type	Description
certificate	No	String	Definition: Specifies the certificate content. It supports certificate chains with a maximum of 11 layers (including certificates and certificate chains). Constraints: N/A Range: The value must be PEM encoded, and can contain a maximum of 65536 characters. Default value: N/A
description	No	String	Definition: Provides supplementary information about the certificate. Constraints: N/A Range: 0 to 255 characters. Default value: N/A
name	No	String	Definition: Specifies the certificate name. Constraints: N/A Range: 0 to 255 characters. Default value: N/A
private_key	No	String	Definition: Specifies the private key of the server certificate. Constraints: N/A Range: The value must be PEM encoded, and can contain a maximum of 8,192 characters. Default value: N/A

Parameter	Mandatory	Type	Description
domain	No	String	Definition: Specifies the domain names used by the server certificate. Constraints: This parameter will take effect only when type is set to server. (For other types of certificates, this parameter can be specified but does not take effect.) Range: 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 Default value: N/A
enc_certificate	No	String	Definition: Specifies the content of the server SM certificate. It supports certificate chains with a maximum of 11 layers (including certificates and certificate chains). Constraints: This parameter is supported only when type is set to server_sm. Range: The value must be PEM encoded, and can contain a maximum of 65,536 characters. Default value: N/A

Parameter	Mandatory	Type	Description
enc_private_key	No	String	Definition: Specifies the private key of the server SM certificate. Constraints: This parameter is supported only when type is set to server_sm . Range: The value must be PEM encoded, and can contain a maximum of 8,192 characters. Default value: N/A
scm_certificate_id	No	String	Definition: Specifies the ID of the certificate managed on Cloud Certificate Manager (CCM). Constraints: The system records only the certificate ID but does not verify its existence on CCM. In addition, you need to update the content of the corresponding certificate on CCM to the related parameters (certificate , private_key , enc_certificate , and enc_private_key) of the current API. Range: N/A Default value: N/A
source	No	String	Definition: Specifies the source of the certificate. Constraints: none Range: • scm: certificates from CCM • Empty: self-signed certificates Default value: N/A

Parameter	Mandatory	Type	Description
protection_status	No	String	Definition: Specifies the protection status. Constraints: N/A Range: • nonProtection: The resource is not protected. • consoleProtection: Modification is not allowed on the console. Default value: N/A
protection_reason	No	String	Definition: Specifies why modification protection is enabled. Constraints: This parameter is valid only when protection_status is set to consoleProtection . Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-211 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
certificate	CertificateInfo object	Definition: Specifies the certificate information. The certificate is defined by the sub-parameter.

Table 5-212 CertificateInfo

Parameter	Type	Description
admin_state_up	Boolean	Definition: Specifies the administrative status of the certificate. This parameter does not take effect whether it is set to true or false . Range: • true: The certificate is available. • false: The certificate is unavailable.
certificate	String	Definition: Specifies the certificate content. It supports certificate chains with a maximum of 11 layers (including certificates and certificate chains). Range: The value must be PEM encoded, and can contain a maximum of 65,536 characters.
description	String	Definition: Provides supplementary information about the certificate. Range: 0 to 255 characters.
domain	String	Definition: Specifies the domain names used by the server certificate. Range: 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	Definition: Specifies the certificate ID. Range: The value consists of 32 digits and lowercase letters.

Parameter	Type	Description
name	String	Definition: Specifies the certificate name. Range: 0 to 255 characters.
private_key	String	Definition: Specifies the private key of the server certificate. Range: The value must be PEM encoded, and can contain a maximum of 8,192 characters.
type	String	Definition: Specifies the certificate type. Range: • server: server certificates • client CA certificates • server_sm: server SM certificates
created_at	String	Definition: Specifies the creation time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.
updated_at	String	Definition: Specifies the update time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.
expire_time	String	Definition: Specifies the time when the certificate expires. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.
project_id	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Range: The value can contain a maximum of 32 characters, including digits and lowercase letters.
enc_certificate	String	Definition: Specifies the content of the server SM certificate. It supports certificate chains with a maximum of 11 layers (including certificates and certificate chains). Range: The value must be PEM encoded, and can contain a maximum of 65536 characters.

Parameter	Type	Description
enc_private_key	String	Definition: Specifies the private key of the server SM certificate. Range: The value must be PEM encoded, and can contain a maximum of 8,192 characters.
scm_certificate_id	String	Definition: Specifies the ID of the certificate managed on Cloud Certificate Manager (CCM). Range: N/A
common_name	String	Definition: Specifies the primary domain name of the certificate. Range: N/A
fingerprint	String	Definition: Specifies the fingerprint of the certificate. Range: N/A
subject_alternative_names	Array of strings	Definition: Specifies all the domain names of the certificate. Range: N/A
source	String	Definition: Specifies the source of the certificate. Range: • scm: certificates from CCM • Empty: self-signed certificates
protection_status	String	Definition: Specifies the protection status. Range: • nonProtection: The resource is not protected. • consoleProtection: Modification is not allowed on the console.
protection_reason	String	Definition: Specifies why modification protection is enabled. Range: N/A

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-----  
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQQDQVAbOLe5xNf4M253Wn9vhdUzojetjv4J  
+B7kYwsMhRcgdcJ8KCnX1nfzTvl2ksXLTQ2o9BkpStnPetB4s32ZiJRMlk  
+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rMMD30gLh6QoP3cq7PGWcuZKV7hjd1tjCT  
QukwMvqV8lqc39buNplgDOWzEP5AzqXtCOFYn6RTH5SRug4hKNN7sT1eYMSlHu7wtEBDKVgrLjOCe/  
W2f8rLT1zEsoAW2ChLZAPYUBkl/0XuTWRg3CohPPcl+UtlRSfVLDeeQ460swjbgwS/RbJh3slwLCRLU08kEo04Z9H/  
AgMBAAECggEAEleaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/  
HlfvCArftGgMaYWPSONCJRMXB7tPwpQu19esjz4Z/  
cR2Je4FTLPrffGUsHFGZjv5OQBZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8ISETq8YaXngBO6vES9LMhHkNK  
Krciu9YkInNEHu6uRJ5g/eGGX3KQynTvVlhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9MEGpfYI6AdHlwFZcT/  
RNAxhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7AlekrguPtFv1vWklg  
+bUFhgGaiAEYTpAUN9t2DVliigQKBgQDnYMMsaF0r557CM1CTXUggCZ08MKeV2jf2drLxRRwRL33SksQbzAQ/  
qrLdT7GP3sCGqvKxWY2FPdFYf8kxGcZPcleZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/  
fbwjpjP7dtJ7n8EzkRUNE6aIMHOFEEych/  
PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYk4aLriWgTWHXPZxUqaYhpjXo6+IMI6DpExiDgBAkMzJGlvS7y  
QiYWU  
+wthAr9urbWYdGZIS6VjoTkF6r7VZoLXX0fbuXh6lm8K8lQRfBpJff56p9phMwaBpDNDrfpHB5utBUxs40yldp6w  
KBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zf3bGSXU/jR4eB1lVQhELG9CbKsDzKM71GyElmix/  
T7FnJSHIWh01qVo6AQyduNWnAQD15pr8KAdXGXAZZ1FQcb3KYa  
+2ffIERmazdOTwJY20tGqZnXkEeMdSLkmqlCRigWhGQKBgDak/735uP20KKqhNehZpC2dJei7OilRhCS/  
dKASUXHSW4fptBnUxACYocdDxtY4Vhaf17FPMdvG8ioYbvlHFh+X0Xs9r1S8yeWnHoXMB6eXWmYKMrAoveLa  
+2cFm1Agf7nLhA4R4lqm9lpV6SKegDUK4fxp9pPyodZPqBLLAoGBAJkD4wHW54PwD4Ctfk9ojHjWB7pQUiYpT  
ZO9dm  
+4fpCMn9Okf43AE2yAOaAP94GdzdJkxfciXKcsYr9lIukfaoXgjKR7p1zERiWZuFF63SB4iayX1H7IX0MwHDZQO3  
8a5gZaOm/BUIGKMWXzuEd3fy+1rCUwzOp9LSjtUYf4ege-----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-----  
MIIC4TCCAcmgAwIBAgICEREwDQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXIDb21wYy55IENBMB4X  
DTE4MDcwMjEzMTU0N1oXDTQ1MTEExNzEzMjU0N1owFDESMBAGA1UEAwWJbG9jYWxob3N0M0M0IIBIjANBgkqh  
kiG9w0BAQEFAAOCAQ8AMIIBCGKCAQEA0FQZi3ucTX+DNud1p/  
b4XVM6I3rY7+Cfge5GMLDIUHXfCgP19Z3807yNpLF5U0NqPQZKURz3rQeLN9mYiUTJZPutYIFDDbB8CtIgV  
+eyU9yJslWx/Bm5kWNPh97B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwkOLpMDL6lfCHKt/  
W7jaSiAazsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQyLYKy4zgnv1tn/  
Ky09cxLKAftgoZWQD2FAZJf9F7k1kYNwqITz3CPILZUUn7yw3nkOotLMI28IEv0WyYd7CMJQks1NPJBKNOGfR/  
wIDAQABozowODAHBgNVHREEGjAYggpkb21haW4uY29thwQKuUvJhwR/  
AAABMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCsGSIb3DQEBCwUAA4IBAQA8IMQJxaTey7EjXtRLSVL  
EAMftAQPG6jjjNQuvIBQYUDauDT4W2XUZ5wAnjiOyQ83va672K1G9s8n6xlH  
+xwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDaezmzCwQYtHBMVQ4c7ML8554Ft1mWSt4dMAK2rzNYjvPR  
LYlp1Hmnl6hkjPk4PCZwKnha0dlScati9Cct3UzXSNJOSLaKdHErH08lqd+1BchScxk0xNITn1HZZGml  
+vbmunok3A2luc14rnsrckbGyqGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZiYsGDVN+9QBd0eYUHce  
+77s96i3l-----END CERTIFICATE-----",  
    "admin_state_up" : true,  
    "project_id" : "99a3ff0d03c428eac3678da6a7d0f24",  
    "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 huaweicloudskgelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskgelb.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 a certificate. If you delete a certificate from CCM, the certificate will only be deleted from the ELB console, but not from the CCM console. To delete a certificate associated with a listener, you need to unbind the certificate from the listener first.

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 5-213 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
certificate_id	Yes	String	Specifies a certificate ID.

Request Parameters

Table 5-214 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 204

Successful request.

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.getStatusCode());  
            System.out.println(e.getRequestId());  
            System.out.println(e.getErrorCode());  
            System.out.println(e.getErrMsg());  
        }  
    }  
}
```

```
}  
}
```

Python

```
# coding: utf-8  
  
import os  
from huaweicloudsdkcore.auth.credentials import BasicCredentials  
from huaweicloudskelb.v3.region.elb_region import ElbRegion  
from huaweicloudsdkcore.exceptions import exceptions  
from huaweicloudskelb.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**. **private_key_echo** defines whether to include **private_key** and **enc_private_key** in the response to each certificate API. If **private_key_echo** is set to **true**, the private key is returned when APIs are called to create a certificate, update a certificate, query the certificate details, and query the certificate list. If **private_key_echo** is set to **false**, the private key is anonymized as ********* and returned. The **private_key_echo** setting applies to the whole tenant project. It is enabled by default.

Calling Method

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

URI

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

Table 5-215 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-216 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-217 Request body parameters

Parameter	Mandatory	Type	Description
private_key_echo	Yes	Boolean	Definition: Specifies whether to set private_key_echo to true . Constraints: N/A Range: • true: The private key is displayed in the responses of the APIs for querying, adding, and updating a certificate, as well as the API for querying the certificate list. • false: The private key is not displayed in the responses of all certificate APIs, but anonymized as ****. Default value: N/A

Response Parameters

Status code: 201

Table 5-218 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
private_key_echo	Boolean	Definition: Specifies whether to set private_key_echo to true . Range: • true: The private key is displayed in the responses of the APIs for querying, adding, and updating a certificate, as well as the API for querying the certificate list. • false: The private key is not displayed in the responses of all certificate APIs, but anonymized as ****.

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

Successful request.

```
{
  "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 huaweicloudskelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskelb.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	Successful request.

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**. This parameter defines whether to include **private_key** and **enc_private_key** in the

response to each certificate API. If **private_key_echo** is set to **true**, the private key is returned. If set to **false**, the private key is anonymized as ********* and returned. The **private_key_echo** setting applies to the whole tenant project. It is enabled by default.

Calling Method

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

URI

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

Table 5-219 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-220 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-221 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
private_key_echo	Boolean	Specifies whether private_key_echo is enabled. Range: • true: The private key is displayed in the responses of the APIs for querying, adding, and updating a certificate, as well as the API for querying the certificate list. • false: The private key is not displayed in the responses of all certificate APIs, but anonymized as *****.

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

Successful request.

```
{
  "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.getStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from 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	Successful request.

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 or TLS listener to your load balancer.

Calling Method

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

URI

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

Table 5-222 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-223 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-224 Request body parameters

Parameter	Mandatory	Type	Description
security_policy	Yes	CreateSecurityPolicyOption object	Definition: Specifies the parameters for creating a custom security policy. Constraints: N/A

Table 5-225 CreateSecurityPolicyOption

Parameter	Mandatory	Type	Description
name	No	String	Definition: Specifies the name of the custom security policy. Constraints: N/A Range: 0 to 255 characters. Default value: N/A
description	No	String	Definition: Specifies the description of the custom security policy. Constraints: N/A Range: 0 to 255 characters. Default value: N/A

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Definition: Specifies the ID of the enterprise project. If no enterprise project ID is specified during resource creation, 0 is returned, indicating that the resource belongs to the default enterprise project. Constraints: The enterprise project ID cannot be "", 0, or an enterprise project ID that does not exist. Range: N/A Default value: 0
protocols	Yes	Array of strings	Definition: Lists the TLS protocols supported by the custom security policy. Constraints: N/A Range: TLSv1, TLSv1.1, TLSv1.2, or TLSv1.3. Default value: N/A

Parameter	Mandatory	Type	Description
ciphers	Yes	Array of strings	Definition: Lists the cipher suites supported by the custom security policy. Constraints: The protocol and cipher suite must match. At least one cipher suite must match the protocol. Range: 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 Default value: N/A NOTE You can match the protocol and cipher suite based on system security policy.

Response Parameters

Status code: 201

Table 5-226 Response body parameters

Parameter	Type	Description
security_policy	SecurityPolicy object	Definition: Specifies the custom security policy information.
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

Table 5-227 SecurityPolicy

Parameter	Type	Description
id	String	Definition: Specifies the ID of the custom security policy. Range: N/A
project_id	String	Definition: Specifies the project ID of the custom security policy. Range: N/A
name	String	Definition: Specifies the name of the custom security policy. Range: N/A
description	String	Definition: Provides supplementary information about the custom security policy. Range: N/A
listeners	Array of ListenerRef objects	Definition: Specifies the listeners that use the custom security policies.
protocols	Array of strings	Definition: Lists the TLS protocols supported by the custom security policy. Range: N/A
ciphers	Array of strings	Definition: Lists the cipher suites supported by the custom security policy. Range: N/A

Parameter	Type	Description
created_at	String	Definition: Specifies the creation time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.
updated_at	String	Definition: Specifies the update time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.

Table 5-228 ListenerRef

Parameter	Type	Description
id	String	Definition: Specifies the listener ID. Range: N/A

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

Successful request.

```
{
  "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	Successful request.

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 5-229 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Table 5-230 Query Parameters

Parameter	Mandatory	Type	Description
marker	No	String	Definition: Specifies the ID of the last record on the previous page. Constraints: • This parameter must be used together with limit. • If the parameter is not specified, only resources on the first page are queried. • This parameter cannot be left blank or set to an invalid ID. Range: N/A Default value: N/A
limit	No	Integer	Definition: Specifies the number of records returned on each page. Constraints: N/A Range: 0 to 2000 Default value: 2000

Parameter	Mandatory	Type	Description
page_reverse	No	Boolean	Definition: Specifies whether to use reverse query. Constraints: • This parameter must be used together with limit. • If page_reverse is set to true and you want to query the resources on the previous page, set the value of marker to the value of previous_marker. Range: • true: Query resources on the previous page. • false: Query resources on the next page. Default value: false
id	No	Array of strings	Definition: Specifies the ID of the custom security policy. Multiple IDs can be used for query in the format of <i>id=xxx&id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
name	No	Array of strings	Definition: Specifies the name of the custom security policy. Multiple names can be used for query in the format of <i>name=xxx&name=xxx</i> . Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
description	No	Array of strings	Definition: Specifies the description of the custom security policy. Multiple descriptions can be used for query in the format of <i>description=xxx&description=xx</i> . Constraints: N/A Range: N/A Default value: N/A
protocols	No	Array of strings	Definition: Specifies the TLS protocols of the custom security policy. Multiple protocols are separated by spaces. Multiple protocols can be used for query in the format of <i>protocols=xxx&protocols=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
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 used for query in the format of <i>ciphers=xxx&ciphers=xxx</i> . Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-231 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200**Table 5-232** Response body parameters

Parameter	Type	Description
security_policies	Array of SecurityPolicy objects	Definition: Lists the security policies.
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
page_info	PageInfo object	Definition: Specifies the pagination information.

Table 5-233 SecurityPolicy

Parameter	Type	Description
id	String	Definition: Specifies the ID of the custom security policy. Range: N/A
project_id	String	Definition: Specifies the project ID of the custom security policy. Range: N/A
name	String	Definition: Specifies the name of the custom security policy. Range: N/A

Parameter	Type	Description
description	String	Definition: Provides supplementary information about the custom security policy. Range: N/A
listeners	Array of ListenerRef objects	Definition: Specifies the listeners that use the custom security policies.
protocols	Array of strings	Definition: Lists the TLS protocols supported by the custom security policy. Range: N/A
ciphers	Array of strings	Definition: Lists the cipher suites supported by the custom security policy. Range: N/A
created_at	String	Definition: Specifies the creation time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.
updated_at	String	Definition: Specifies the update time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.

Table 5-234 ListenerRef

Parameter	Type	Description
id	String	Definition: Specifies the listener ID. Range: N/A

Table 5-235 PageInfo

Parameter	Type	Description
previous_marker	String	Definition: Specifies the ID of the first record in the pagination query result. If page_reverse is set to true , this parameter is used together to query resources on the previous page. Range: N/A

Parameter	Type	Description
next_marker	String	Definition: Specifies the ID of the last record in the pagination query result. It is usually used to query resources on the next page. Range: N/A
current_count	Integer	Definition: Specifies the number of records returned on the current page. Range: N/A

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 5-236 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
security_policy_id	Yes	String	Specifies the ID of the custom security policy.

Request Parameters

Table 5-237 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-238 Response body parameters

Parameter	Type	Description
security_policy	SecurityPolicy object	Definition: Specifies the custom security policy information.
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

Table 5-239 SecurityPolicy

Parameter	Type	Description
id	String	Definition: Specifies the ID of the custom security policy. Range: N/A
project_id	String	Definition: Specifies the project ID of the custom security policy. Range: N/A
name	String	Definition: Specifies the name of the custom security policy. Range: N/A

Parameter	Type	Description
description	String	Definition: Provides supplementary information about the custom security policy. Range: N/A
listeners	Array of ListenerRef objects	Definition: Specifies the listeners that use the custom security policies.
protocols	Array of strings	Definition: Lists the TLS protocols supported by the custom security policy. Range: N/A
ciphers	Array of strings	Definition: Lists the cipher suites supported by the custom security policy. Range: N/A
created_at	String	Definition: Specifies the creation time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.
updated_at	String	Definition: Specifies the update time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.

Table 5-240 ListenerRef

Parameter	Type	Description
id	String	Definition: Specifies the listener ID. Range: N/A

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 huaweicloudskelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskelb.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 5-241 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
security_policy_id	Yes	String	Specifies the ID of the custom security policy.

Request Parameters

Table 5-242 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-243 Request body parameters

Parameter	Mandatory	Type	Description
security_policy	Yes	UpdateSecurityPolicyOption object	Definition: Specifies the request parameters for updating the custom security policy. Constraints: N/A

Table 5-244 UpdateSecurityPolicyOption

Parameter	Mandatory	Type	Description
name	No	String	Definition: Specifies the name of the custom security policy. Constraints: N/A Range: 0 to 255 characters. Default value: N/A
description	No	String	Definition: Specifies the description of the custom security policy. Constraints: N/A Range: 0 to 255 characters. Default value: N/A
protocols	No	Array of strings	Definition: Lists the TLS protocols supported by the custom security policy. Constraints: N/A Range: TLSv1, TLSv1.1, TLSv1.2, and TLSv1.3. Default value: N/A

Parameter	Mandatory	Type	Description
ciphers	No	Array of strings	Definition: Lists the cipher suites supported by the custom security policy. Constraints: The protocol and cipher suite must match. At least one cipher suite must match the protocol. Range: 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 Default value: N/A NOTE You can match the protocol and cipher suite based on system security policy.

Response Parameters

Status code: 200

Table 5-245 Response body parameters

Parameter	Type	Description
security_policy	SecurityPolicy object	Definition: Specifies the custom security policy. Constraints: N/A
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

Table 5-246 SecurityPolicy

Parameter	Type	Description
id	String	Definition: Specifies the ID of the custom security policy. Range: N/A
project_id	String	Definition: Specifies the project ID of the custom security policy. Range: N/A
name	String	Definition: Specifies the name of the custom security policy. Range: N/A
description	String	Definition: Provides supplementary information about the custom security policy. Range: N/A
listeners	Array of ListenerRef objects	Definition: Specifies the listeners that use the custom security policies.
protocols	Array of strings	Definition: Lists the TLS protocols supported by the custom security policy. Range: N/A

Parameter	Type	Description
ciphers	Array of strings	Definition: Lists the cipher suites supported by the custom security policy. Range: N/A
created_at	String	Definition: Specifies the creation time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.
updated_at	String	Definition: Specifies the update time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.

Table 5-247 ListenerRef

Parameter	Type	Description
id	String	Definition: Specifies the listener ID. Range: N/A

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.setName("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.getErrMsg());
}
}
```

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 5-248 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
security_policy_id	Yes	String	Specifies the ID of the custom security policy.

Request Parameters

Table 5-249 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 204

Successful request.

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 5-250 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-251 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-252 Response body parameters

Parameter	Type	Description
system_security_policies	Array of SystemSecurityPolicy objects	Definition: Lists system security policies.
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

Table 5-253 SystemSecurityPolicy

Parameter	Type	Description
name	String	Definition: Specifies the name of the system security policy. Range: N/A
protocols	String	Definition: Lists the TLS protocols supported by the system security policy. Range: N/A
ciphers	String	Definition: Lists the cipher suites supported by the system security policy. Range: N/A

Parameter	Type	Description
project_id	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Range: The value can contain a maximum of 32 characters, including digits and lowercase letters.

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"
  } ]
}
```

```
SHA384:ECDSA-RSA-AES256-SHA:ECDSA-RSA-AES256-SHA:AES128-SHA:AES256-SHA"
}, {
  "name": "tls-1-2-strict",
  "project_id": "7a9941d34fc1497d8d0797429ecfd354",
  "protocols": "TLSv1.2",
  "ciphers": "ECDHE-ECDSA-AES256-GCM-SHA384:ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES128-SHA256:ECDSA-AES256-SHA384:ECDSA-AES128-GCM-SHA256:ECDSA-AES256-
GCM-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDSA-AES128-SHA256:AES128-
SHA256:AES256-SHA256:ECDSA-AES256-SHA384"
}, {
  "name": "tls-1-2-fs",
  "project_id": "7a9941d34fc1497d8d0797429ecfd354",
  "protocols": "TLSv1.2",
  "ciphers": "ECDHE-ECDSA-AES256-GCM-SHA384:ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES128-SHA256:ECDSA-AES256-SHA384:ECDSA-AES128-GCM-SHA256:ECDSA-AES256-
GCM-SHA256:ECDSA-AES128-SHA256:ECDSA-AES256-SHA384:ECDSA-AES128-
GCM-SHA256:ECDSA-AES128-SHA256:ECDSA-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:ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES128-SHA256:ECDSA-AES256-SHA384:ECDSA-AES128-SHA:ECDSA-AES256-
SHA:ECDSA-RSA-AES256-GCM-SHA384:ECDSA-RSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-
GCM-SHA384:ECDSA-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDSA-RSA-AES256-
SHA384:ECDSA-RSA-AES128-SHA:ECDSA-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:ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES128-SHA256:ECDSA-AES256-SHA384:ECDSA-RSA-AES256-GCM-SHA384:ECDSA-RSA-AES128-
GCM-SHA256:ECDSA-RSA-AES128-SHA256:ECDSA-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:ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES128-SHA256:ECDSA-AES256-SHA384:ECDSA-AES128-SHA:ECDSA-AES256-
SHA:ECDSA-RSA-AES256-GCM-SHA384:ECDSA-RSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES256-
GCM-SHA384:ECDSA-RSA-AES128-SHA256:AES128-SHA256:AES256-SHA256:ECDSA-RSA-AES256-
SHA384:ECDSA-RSA-AES128-SHA:ECDSA-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:ECDSA-AES128-GCM-SHA256:ECDSA-RSA-
AES256-GCM-SHA384:ECDSA-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.getStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from 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.getenv("CLOUD_SDK_AK")
    sk = os.getenv("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. You can associate the IP address group with a listener to control access to this listener.

Each IP address group can contain IP addresses, IP address ranges, and 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.

Note: 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, either one will be kept. 0:0:0:0:0:0:1 will be considered the same as ::1 and ::1/128. If you enter 0:0:0:0:0:0:1, ::1, and ::1/128, only one will be kept.

Calling Method

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

URI

POST /v3/{project_id}/elb/ipgroups

Table 5-254 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-255 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-256 Request body parameters

Parameter	Mandatory	Type	Description
ipgroup	Yes	CreateIpGroupOption object	Definition: Specifies the request parameters for creating an IP address group. Constraints: N/A

Table 5-257 CreateIpGroupOption

Parameter	Mandatory	Type	Description
project_id	No	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A NOTE This parameter is invalid. The project ID in the URL is used.
description	No	String	Definition: Provides supplementary information about an IP address group. Constraints: N/A Range: 0 to 255 characters. Default value: N/A

Parameter	Mandatory	Type	Description
name	No	String	Definition: Specifies the name of an IP address group. Constraints: N/A Range: 0 to 255 characters. Default value: N/A
ip_list	Yes	Array of CreateIpGroupIpOption objects	Definition: Specifies entries in the IP address group. Both IPv4 and IPv6 entries are supported. Constraints: N/A
enterprise_project_id	No	String	Definition: Specifies the ID of the enterprise project. If no enterprise project ID is specified during resource creation, 0 is returned, indicating that the resource belongs to the default enterprise project. Constraints: The enterprise project ID cannot be "", 0, or an enterprise project ID that does not exist. Range: N/A Default value: 0

Table 5-258 CreateIpGroupIpOption

Parameter	Mandatory	Type	Description
ip	Yes	String	Definition: Specifies the IP entries in the IP address group. Constraints: N/A Range: Each entry can be an IP address, IP address range, or CIDR block. Each IP address range must be in the format of <i>ip-ip</i> , for example, 192.168.1.2-192.168.2.253 or 2001:0DB8:02de::0e12-2001:0DB8:02de::0e13. Both IPv4 and IPv6 addresses are supported. Default value: N/A

Parameter	Mandatory	Type	Description
description	No	String	Definition: Specifies remarks about the IP address group. Constraints: N/A Range: 0 to 255 characters. Default value: N/A

Response Parameters

Status code: 201

Table 5-259 Response body parameters

Parameter	Type	Description
ipgroup	IpGroup object	Definition: Specifies the response body for creating an IP address group.
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

Table 5-260 IpGroup

Parameter	Type	Description
id	String	Definition: Specifies the ID of an IP address group. Range: N/A
name	String	Definition: Specifies the name of an IP address group. Range: N/A
description	String	Definition: Provides supplementary information about an IP address group. Range: N/A
ip_list	Array of IpInfo objects	Definition: Specifies IP addresses in an IP address group. [] indicates any IP address.
listeners	Array of ListenerRef objects	Definition: Specifies the IDs of listeners with which the IP address group is associated.

Parameter	Type	Description
project_id	String	Definition: Specifies the project ID of the IP address group. Range: N/A
enterprise_project_id	String	Definition: Specifies the ID of the enterprise project. Range: • 0: The resource belongs to the default enterprise project. • A string in UUID format indicates a non-default enterprise project.
created_at	String	Definition: Specifies the time when the IP address group was created. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.
updated_at	String	Definition: Specifies the time when the IP address group was updated. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.

Table 5-261 IpInfo

Parameter	Type	Description
ip	String	Definition: Specifies the IP entries in the IP address group. Range: Each IP address range must be in the format of <i>ip-ip</i> , 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	String	Definition: Provides remarks about the IP address group. Range: 0 to 255 characters.

Table 5-262 ListenerRef

Parameter	Type	Description
id	String	Definition: Specifies the listener ID. Range: N/A

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.setName("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.getStatusCode());
        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 5-263 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Table 5-264 Query Parameters

Parameter	Mandatory	Type	Description
marker	No	String	Definition: Specifies the ID of the last record on the previous page. Constraints: • This parameter must be used together with limit. • If the parameter is not specified, only resources on the first page are queried. • This parameter cannot be left blank or set to an invalid ID. Range: N/A Default value: N/A
limit	No	Integer	Definition: Specifies the number of records returned on each page. Constraints: N/A Range: 0 to 2000 Default value: 2000

Parameter	Mandatory	Type	Description
page_reverse	No	Boolean	Definition: Specifies whether to use reverse query. Constraints: • This parameter must be used together with limit. • If page_reverse is set to true and you want to query the resources on the previous page, set the value of marker to the value of previous_marker. Range: • true: Query resources on the previous page. • false: Query resources on the next page. Default value: false
id	No	Array of strings	Definition: Specifies the ID of an IP address group. Constraints: N/A Range: N/A Default value: N/A
name	No	Array of strings	Definition: Specifies the name of an IP address group. Constraints: N/A Range: N/A Default value: N/A
description	No	Array of strings	Definition: Provides supplementary information about an IP address group. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
ip_list	No	Array of strings	Definition: Specifies one or more IP entries for querying IP address groups. If you enter multiple IP entries, the system searches for all IP address groups containing any of the IP entries. Note: All IP addresses, CIDR blocks, and IP address ranges are searched using exact matches. For example, if an IP address group has the IP address range 127.0.0.1-127.0.0.10, you need to set ip_list to 127.0.0.1-127.0.0.10. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
enterprise_project_id	No	Array of strings	Definition: Specifies the ID of the enterprise project. Multiple values can be used for query in the format of: <i>enterprise_project_id=xxx&enterprise_project_id=xxx.</i> Constraints: • 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. Range: N/A Default value: N/A

Request Parameters

Table 5-265 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-266 Response body parameters

Parameter	Type	Description
ipgroups	Array of IpGroup objects	Definition: Lists the returned IP address groups.
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
page_info	PageInfo object	Definition: Specifies the pagination information.

Table 5-267 IpGroup

Parameter	Type	Description
id	String	Definition: Specifies the ID of an IP address group. Range: N/A
name	String	Definition: Specifies the name of an IP address group. Range: N/A
description	String	Definition: Provides supplementary information about an IP address group. Range: N/A
ip_list	Array of IpInfo objects	Definition: Specifies IP addresses in an IP address group. [] indicates any IP address.
listeners	Array of ListenerRef objects	Definition: Specifies the IDs of listeners with which the IP address group is associated.
project_id	String	Definition: Specifies the project ID of the IP address group. Range: N/A

Parameter	Type	Description
enterprise_project_id	String	Definition: Specifies the ID of the enterprise project. Range: • 0: The resource belongs to the default enterprise project. • A string in UUID format indicates a non-default enterprise project.
created_at	String	Definition: Specifies the time when the IP address group was created. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.
updated_at	String	Definition: Specifies the time when the IP address group was updated. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.

Table 5-268 IpInfo

Parameter	Type	Description
ip	String	Definition: Specifies the IP entries in the IP address group. Range: Each IP address range must be in the format of <i>ip-ip</i> , 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	String	Definition: Provides remarks about the IP address group. Range: 0 to 255 characters.

Table 5-269 ListenerRef

Parameter	Type	Description
id	String	Definition: Specifies the listener ID. Range: N/A

Table 5-270 PageInfo

Parameter	Type	Description
previous_marker	String	Definition: Specifies the ID of the first record in the pagination query result. If page_reverse is set to true , this parameter is used together to query resources on the previous page. Range: N/A
next_marker	String	Definition: Specifies the ID of the last record in the pagination query result. It is usually used to query resources on the next page. Range: N/A
current_count	Integer	Definition: Specifies the number of records returned on the current page. Range: N/A

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 5-271 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Parameter	Mandatory	Type	Description
ipgroup_id	Yes	String	Definition: Specifies the ID of an IP address group.

Request Parameters

Table 5-272 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-273 Response body parameters

Parameter	Type	Description
ipgroup	IpGroup object	Definition: Specifies the response body for querying the details of the IP address group.
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

Table 5-274 IpGroup

Parameter	Type	Description
id	String	Definition: Specifies the ID of an IP address group. Range: N/A
name	String	Definition: Specifies the name of an IP address group. Range: N/A

Parameter	Type	Description
description	String	Definition: Provides supplementary information about an IP address group. Range: N/A
ip_list	Array of IpInfo objects	Definition: Specifies IP addresses in an IP address group. [] indicates any IP address.
listeners	Array of ListenerRef objects	Definition: Specifies the IDs of listeners with which the IP address group is associated.
project_id	String	Definition: Specifies the project ID of the IP address group. Range: N/A
enterprise_project_id	String	Definition: Specifies the ID of the enterprise project. Range: • 0: The resource belongs to the default enterprise project. • A string in UUID format indicates a non-default enterprise project.
created_at	String	Definition: Specifies the time when the IP address group was created. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.
updated_at	String	Definition: Specifies the time when the IP address group was updated. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.

Table 5-275 IpInfo

Parameter	Type	Description
ip	String	Definition: Specifies the IP entries in the IP address group. Range: Each IP address range must be in the format of <i>ip-ip</i> , 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.

Parameter	Type	Description
description	String	Definition: Provides remarks about the IP address group. Range: 0 to 255 characters.

Table 5-276 ListenerRef

Parameter	Type	Description
id	String	Definition: Specifies the listener ID. Range: N/A

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

Definition: 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	Definition: 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 entries in the IP address group will be overwritten, and those that are not included in the **ip_list** parameter in the request body will be removed.

Each IP address group can contain single IP addresses, IP address ranges, and CIDR blocks. Both IPv4 and IPv6 addresses are supported. Each IP address range must be in the format of *ip-ip*, for example, 10.12.3.1-10.12.3.10.

Note:

- 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, either one will be kept. 0:0:0:0:0:0:1 will be considered the same as ::1 and ::1/128. If you enter 0:0:0:0:0:0:1, ::1, and ::1/128, only one will be kept.
- Updating the entries defined by **ip_list** will affect all associated listeners.

Calling Method

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

URI

PUT /v3/{project_id}/elb/ipgroups/{ipgroup_id}

Table 5-277 Path Parameters

Parameter	Mandatory	Type	Description
ipgroup_id	Yes	String	Definition: Specifies the ID of the IP address group to be updated. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-278 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-279 Request body parameters

Parameter	Mandatory	Type	Description
ipgroup	Yes	UpdateIpGroupOption object	Definition: Specifies the request parameters for updating an IP address group. Constraints: N/A

Table 5-280 UpdateIpGroupOption

Parameter	Mandatory	Type	Description
description	No	String	Definition: Provides supplementary information about an IP address group. Constraints: N/A Range: 0 to 255 characters. Default value: N/A

Parameter	Mandatory	Type	Description
name	No	String	Definition: Specifies the name of an IP address group. Constraints: N/A Range: 0 to 255 characters. Default value: N/A
ip_list	No	Array of UpdateIpGroupIpOption objects	Definition: Specifies one or more IP entries for the IP address group. Note: All IP entries in the IP address group will be overwritten, and those that are not included in the ip_list parameter in the request body will be removed. Constraints: N/A

Table 5-281 UpdateIpGroupIpOption

Parameter	Mandatory	Type	Description
ip	Yes	String	Definition: Specifies the IP entries in the IP address group. Constraints: N/A Range: Each entry can be an IP address, IP address range, or CIDR block. Each IP address range must be in the format of <i>ip-ip</i> , for example, 192.168.1.2-192.168.2.253 or 2001:0DB8:02de::0e12-2001:0DB8:02de::0e13. Both IPv4 and IPv6 addresses are supported. Default value: N/A
description	No	String	Definition: Specifies remarks about the IP address group. Constraints: N/A Range: 0 to 255 characters. Default value: N/A

Response Parameters

Status code: 200

Table 5-282 Response body parameters

Parameter	Type	Description
ipgroup	IpGroup object	Definition: Specifies the IP address group information.
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

Table 5-283 IpGroup

Parameter	Type	Description
id	String	Definition: Specifies the ID of an IP address group. Range: N/A
name	String	Definition: Specifies the name of an IP address group. Range: N/A
description	String	Definition: Provides supplementary information about an IP address group. Range: N/A
ip_list	Array of IpInfo objects	Definition: Specifies IP addresses in an IP address group. [] indicates any IP address.
listeners	Array of ListenerRef objects	Definition: Specifies the IDs of listeners with which the IP address group is associated.
project_id	String	Definition: Specifies the project ID of the IP address group. Range: N/A
enterprise_project_id	String	Definition: Specifies the ID of the enterprise project. Range: • 0: The resource belongs to the default enterprise project. • A string in UUID format indicates a non-default enterprise project.

Parameter	Type	Description
created_at	String	Definition: Specifies the time when the IP address group was created. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.
updated_at	String	Definition: Specifies the time when the IP address group was updated. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.

Table 5-284 IpInfo

Parameter	Type	Description
ip	String	Definition: Specifies the IP entries in the IP address group. Range: Each IP address range must be in the format of <i>ip-ip</i> , 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	String	Definition: Provides remarks about the IP address group. Range: 0 to 255 characters.

Table 5-285 ListenerRef

Parameter	Type	Description
id	String	Definition: Specifies the listener ID. Range: N/A

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 UpdatelpGroupSolution {

  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<UpdateIpGroupIpOption> listIpGroupIpList = new ArrayList<>();
listIpGroupIpList.add(
    new UpdateIpGroupIpOption()
        .withIp("192.168.1.123")
);
listIpGroupIpList.add(
    new UpdateIpGroupIpOption()
        .withIp("192.168.3.0/24")
        .withDescription("test_ip")
);
UpdateIpGroupOption ipgroupbody = new UpdateIpGroupOption();
ipgroupbody.setName("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 = [
        UpdateIpGroupIpOption(
            ip="192.168.1.123"
        ),
        UpdateIpGroupIpOption(
            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.UpdateIpGroupIpOption{
    {
        Ip: "192.168.1.123",
    },
    {
        Ip: "192.168.3.0/24",
        Description: &descriptionIpList,
    },
}
namelpgroup:= "test_ipg"
ipgroupbody := &model.UpdateIpGroupOption{
    Name: &namelpgroup,
    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. An IP address group that has been associated with a listener cannot be deleted. You need to disassociate the IP address group first.

Calling Method

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

URI

DELETE /v3/{project_id}/elb/ipgroups/{ipgroup_id}

Table 5-286 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
ipgroup_id	Yes	String	Definition: Specifies the ID of an IP address group.

Request Parameters

Table 5-287 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 204

Definition: Normal response to the DELETE operation.

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 DeletelpGroupSolution {

    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();
        DeletelpGroupRequest request = new DeletelpGroupRequest();
        request.withIpgroupId("{ipgroup_id}");
        try {
            DeletelpGroupResponse response = client.deletelpGroup(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 = DeletelpGroupRequest()
        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.ElClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.DeletelpGroupRequest{}
    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	Definition: Normal response to the DELETE operation.

Error Codes

See [Error Codes](#).

5.9.6 Updating IP Addresses in an IP Address Group

Function

This API is used to add IP addresses to an IP address group, or update the descriptions of existing IP addresses. This API cannot be used to delete IP addresses.

Note:

- 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, either one will be kept. 0:0:0:0:0:0:1 will be considered the same as ::1 and ::1/128. If you enter 0:0:0:0:0:0:1, ::1, and ::1/128, only one will be kept.
- Updating the entries defined by **ip_list** will affect all associated listeners.

Calling Method

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

URI

POST /v3/{project_id}/elb/ipgroups/{ipgroup_id}/iplist/create-or-update

Table 5-288 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
ipgroup_id	Yes	String	Definition: Specifies the ID of an IP address group. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-289 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-290 Request body parameters

Parameter	Mandatory	Type	Description
ipgroup	No	UpdateIpListOption object	Definition: Specifies the request parameters for updating IP entries in an IP address group. Constraints: N/A

Table 5-291 UpdateIpListOption

Parameter	Mandatory	Type	Description
name	No	String	Definition: Specifies the name of an IP address group. Constraints: N/A Range: N/A Default value: N/A
ip_list	No	Array of UpdateIpGroupIpOption objects	Definition: Specifies IP entries in an IP address group. The specified IP entries will be added to the IP address group, or the descriptions of existing IP entries will be updated. But the existing IP entries will not be deleted or modified. Constraints: N/A
description	No	String	Definition: Specifies remarks about the IP address group. Constraints: N/A Range: 0 to 255 characters. Default value: N/A

Table 5-292 UpdateIpGroupIpOption

Parameter	Mandatory	Type	Description
ip	Yes	String	Definition: Specifies the IP entries in the IP address group. Constraints: N/A Range: Each entry can be an IP address, IP address range, or CIDR block. Each IP address range must be in the format of <i>ip-ip</i> , for example, 192.168.1.2-192.168.2.253 or 2001:0DB8:02de::0e12-2001:0DB8:02de::0e13. Both IPv4 and IPv6 addresses are supported. Default value: N/A

Parameter	Mandatory	Type	Description
description	No	String	Definition: Specifies remarks about the IP address group. Constraints: N/A Range: 0 to 255 characters. Default value: N/A

Response Parameters

Status code: 200

Table 5-293 Response body parameters

Parameter	Type	Description
ipgroup	IpGroup object	Definition: Specifies the IP address group information.
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

Table 5-294 IpGroup

Parameter	Type	Description
id	String	Definition: Specifies the ID of an IP address group. Range: N/A
name	String	Definition: Specifies the name of an IP address group. Range: N/A
description	String	Definition: Provides supplementary information about an IP address group. Range: N/A
ip_list	Array of IpInfo objects	Definition: Specifies IP addresses in an IP address group. [] indicates any IP address.
listeners	Array of ListenerRef objects	Definition: Specifies the IDs of listeners with which the IP address group is associated.

Parameter	Type	Description
project_id	String	Definition: Specifies the project ID of the IP address group. Range: N/A
enterprise_project_id	String	Definition: Specifies the ID of the enterprise project. Range: • 0: The resource belongs to the default enterprise project. • A string in UUID format indicates a non-default enterprise project.
created_at	String	Definition: Specifies the time when the IP address group was created. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.
updated_at	String	Definition: Specifies the time when the IP address group was updated. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.

Table 5-295 IpInfo

Parameter	Type	Description
ip	String	Definition: Specifies the IP entries in the IP address group. Range: Each IP address range must be in the format of <i>ip-ip</i> , 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	String	Definition: Provides remarks about the IP address group. Range: 0 to 255 characters.

Table 5-296 ListenerRef

Parameter	Type	Description
id	String	Definition: Specifies the listener ID. Range: N/A

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 UpdatelplistSolution {

    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();
        UpdatelplistRequest request = new UpdatelplistRequest();
        request.withIpgroupId("{ipgroup_id}");
        UpdatelplistRequestBody body = new UpdatelplistRequestBody();
        List<UpdatelplistGroupIpOption> listIpgroupIdList = new ArrayList<>();
        listIpgroupIdList.add(
            new UpdatelplistGroupIpOption()
                .withIp("192.168.1.123")
                .withDescription("test")
        );
        listIpgroupIdList.add(
            new UpdatelplistGroupIpOption()
                .withIp("192.168.1.120")
                .withDescription("test update ip0")
        );
        UpdatelplistOption ipgroupbody = new UpdatelplistOption();
        ipgroupbody.withName("test_ipg")
            .withIpList(listIpgroupIdList);
        body.withIpgroup(ipgroupbody);
        request.withBody(body);
        try {
            UpdatelplistResponse response = client.updatelplist(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 = [  
            UpdateIpGroupIpOption(  
                ip="192.168.1.123",  
                description="test"  
            ),  
            UpdateIpGroupIpOption(  
                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.UpdateIpGroupIpOption{
        {
            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.

Note: Deleting IP addresses from an IP address group will affect all associated listeners.

Calling Method

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

URI

POST /v3/{project_id}/elb/ipgroups/{ipgroup_id}/iplist/batch-delete

Table 5-297 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
ipgroup_id	Yes	String	Definition: Specifies the ID of an IP address group. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-298 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-299 Request body parameters

Parameter	Mandatory	Type	Description
ipgroup	No	BatchDeleteIpListOption object	Definition: Specifies the request parameters for deleting IP entries in batches. Constraints: N/A

Table 5-300 BatchDeleteIpListOption

Parameter	Mandatory	Type	Description
ip_list	No	Array of IpGroupIp objects	Definition: Specifies the IP entries in the IP address group. Constraints: N/A

Table 5-301 IpGroupIp

Parameter	Mandatory	Type	Description
ip	Yes	String	Definition: Specifies the IP entries to be deleted from the IP address group. Each IP entry can be a single IP address, CIDR block, or IP address range. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-302 Response body parameters

Parameter	Type	Description
ipgroup	IpGroup object	Definition: Specifies the IP address group information.
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

Table 5-303 IpGroup

Parameter	Type	Description
id	String	Definition: Specifies the ID of an IP address group. Range: N/A
name	String	Definition: Specifies the name of an IP address group. Range: N/A
description	String	Definition: Provides supplementary information about an IP address group. Range: N/A
ip_list	Array of IpInfo objects	Definition: Specifies IP addresses in an IP address group. [] indicates any IP address.
listeners	Array of ListenerRef objects	Definition: Specifies the IDs of listeners with which the IP address group is associated.
project_id	String	Definition: Specifies the project ID of the IP address group. Range: N/A

Parameter	Type	Description
enterprise_project_id	String	Definition: Specifies the ID of the enterprise project. Range: • 0: The resource belongs to the default enterprise project. • A string in UUID format indicates a non-default enterprise project.
created_at	String	Definition: Specifies the time when the IP address group was created. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.
updated_at	String	Definition: Specifies the time when the IP address group was updated. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format.

Table 5-304 IpInfo

Parameter	Type	Description
ip	String	Definition: Specifies the IP entries in the IP address group. Range: Each IP address range must be in the format of <i>ip-ip</i> , 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	String	Definition: Provides remarks about the IP address group. Range: 0 to 255 characters.

Table 5-305 ListenerRef

Parameter	Type	Description
id	String	Definition: Specifies the listener ID. Range: N/A

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 huaweicloudskelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskelb.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 5-306 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
ipgroup_id	Yes	String	Definition: Specifies the ID of an IP address group. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-307 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-308 Response body parameters

Parameter	Type	Description
listeners	Array of ListenerRef objects	Definition: Specifies the IDs of all listeners associated with the IP address group.

Table 5-309 ListenerRef

Parameter	Type	Description
id	String	Definition: Specifies the listener ID. Range: N/A

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

Definition: Successful request.

```
{  
  "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.getenv("CLOUD_SDK_AK")
    sk = os.getenv("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	Definition: Successful request.

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 shared or dedicated 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 5-310 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-311 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-312 Request body parameters

Parameter	Mandatory	Type	Description
listener	Yes	CreateListenerOption object	Definition: Specifies the request parameters for adding a listener. Constraints: N/A

Table 5-313 CreateListenerOption

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Definition: Specifies the administrative status of the listener. Constraints: The value can only be true . Range: true indicates the listener is in use. Default value: true
default_pool_id	No	String	Definition: Specifies the ID of the default backend server group of the listener. If there is no matched forwarding policy, requests will be routed to the default backend server group. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
client_ca_tls_container_ref	No	String	Definition: Specifies the ID of the CA certificate used by the listener. Constraints: • This parameter is available only when type is set to client. • This parameter is not available if the listener protocol is QUIC. • To enable mutual authentication, both client_ca_tls_container_ref and default_tls_container_ref are required. Range: N/A Default value: N/A
default_tls_container_ref	No	String	Definition: Specifies the ID of the server certificate used by the listener. Constraints: • type must be server. • This parameter is mandatory when the listener protocol is HTTPS, TLS, or QUIC. • Both client_ca_tls_container_ref and default_tls_container_ref are required for mutual authentication. Only default_tls_container_ref is required for one-way authentication. Range: N/A Default value: N/A
description	No	String	Definition: Provides supplementary information about the listener. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
http2_enable	No	Boolean	Definition: Specifies whether to allow clients to use HTTP/2 to communicate with the load balancer for higher access performance. However, the load balancer still uses HTTP/1.x to forward requests to backend servers. Constraints: • This parameter is valid only for HTTPS listeners. • This parameter is not available for QUIC listeners and the response is fixed at true. • You can configure this parameter for listeners with other protocols, but it will not take effect. Range: • true: Enable this option. • false: Disable this option. Default value: false
insert_headers	No	ListenerInsertHeaders object	Definition: Specifies the HTTP headers that can transmit required information to backend servers. For example, you can use the X-Forwarded-ELB-IP header to transmit the load balancer EIP to backend servers. Constraints: This parameter can be configured only for HTTP, HTTPS, and QUIC listeners.
loadbalancer_id	Yes	String	Definition: Specifies the ID of the load balancer that the listener is added to. Constraints: A listener can be added to only one load balancer. Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
name	No	String	Definition: Specifies the name of the listener. Note: If you leave the listener name empty, you cannot locate it in the listener list and view its details. Range: The value can contain 0 to 255 characters. Default value: N/A
project_id	No	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A NOTE This parameter is invalid. The project ID in the URL is used.
protocol	Yes	String	Definition: Specifies the protocol of the listener. Constraints: - 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. Range: TCP, UDP, HTTP, HTTPS, TERMINATED_HTTPS, QUIC, or TLS. Default value: N/A

Parameter	Mandatory	Type	Description
protocol_port	No	Integer	Definition: Specifies the port used by the listener. Constraints: • QUIC listeners cannot use port 4789, and cannot use the same port as UDP listeners. • 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. Range: 0 to 65535 Default value: N/A
sni_container_refs	No	Array of strings	Definition: Specifies the IDs of SNI certificates (server certificates with domain names) used by the listener. Constraints: • QUIC listeners support only RSA certificates. • Each domain name of an SNI certificate must be unique. • The total number of domain names of all SNI certificates cannot exceed 200. Range: 0 to 50 Default value: N/A
sni_match_algo	No	String	Definition: Specifies how wildcard domain name matches with the SNI certificates used by the listener. Constraints: N/A Range: • longest_suffix: indicates longest suffix match. • wildcard: indicates wildcard match. Default value: wildcard

Parameter	Mandatory	Type	Description
tags	No	Array of Tag objects	Definition: Lists the tags. Constraints: N/A
tls_ciphers_policy	No	String	Definition: Specifies the security policy used by the listener. Constraints: • This parameter is available 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 takes 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). Range: tls-1-0-inherit, tls-1-0, tls-1-1, tls-1-2, 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. The default value is tls-1-2. Default value: N/A

Parameter	Mandatory	Type	Description
security_policy_id	No	String	Definition: Specifies the ID of the custom security policy. Constraints: • This parameter is available 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 takes 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). Range: N/A Default value: N/A
enable_member_retry	No	Boolean	Definition: Specifies whether to enable health check retries for backend servers. Constraints: • 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. Range: true indicates health check retries will be enabled. false indicates health check retries will be disabled. Default value: true

Parameter	Mandatory	Type	Description
keepalive_timeout	No	Integer	Definition: Specifies the idle timeout duration, in seconds. If the load balancer receives no requests within the idle timeout duration, it will disconnect the connection with the client and establish a new connection when there is a new request. Constraints: This parameter is not supported by UDP listeners of shared load balancers. Range: • For TCP listeners, the value ranges from 10s to 4000s. The default value is 300s. • For HTTP, HTTPS, and TERMINATED_HTTPS listeners, the value ranges from 0s to 4000s. The default value is 60s. Default value: N/A
client_timeout	No	Integer	Definition: 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. Constraints: This parameter is available only for HTTP and HTTPS listeners. Range: 1-300s Default value: 60s

Parameter	Mandatory	Type	Description
member_timeout	No	Integer	Definition: 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. Constraints: This parameter is available only for HTTP and HTTPS listeners. Range: 1-300s Default value: 60s
ipgroup	No	CreateListenerIpGroupOption object	Definition: 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. Constraints: N/A

Parameter	Mandatory	Type	Description
transparent_client_ip_enable	No	Boolean	Definition: Specifies whether to pass source IP addresses of the clients to backend servers. Constraints: • This parameter is available only for TCP and UDP listeners of shared load balancers. • If this function is enabled, the load balancer communicates with backend servers using client 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, the backend server specifications cannot be changed. Range: • 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. Default value: N/A

Parameter	Mandatory	Type	Description
proxy_protocol_enable	No	Boolean	Definition: Specifies whether to enable ProxyProtocol to pass the source IP addresses of the clients to backend servers. Constraints: This parameter is available only for TLS listeners and does not take effect for other types of listeners. Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
enhance_l7policy_enable	No	Boolean	Definition: Specifies whether to enable advanced forwarding. If advanced forwarding is enabled, more flexible forwarding policies and rules are supported. 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. Constraints: • Advanced forwarding cannot be disabled once it is enabled. • If advanced forwarding is enabled, forwarding policy priorities are defined by priority. The priorities are not automatically sorted. For details, see the description of the priority parameter in the forwarding policy.

Parameter	Mandatory	Type	Description
			Range: The value can be true (enable this option) or false (disable this option). Default value: false
quic_config	No	CreateListenerQuicConfigOption object	Definition: Specifies the QUIC configuration for the current listener. Constraints: • 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. NOTE Suppose the client sends an HTTP request to the server and carries information indicating that the QUIC protocol is supported. If enable_quic_upgrade is set to true , the QUIC port and version information supported by the server will be included in the response header. When the client sends both HTTPS and QUIC requests, if the QUIC request is sent and responded, the client will use the QUIC protocol to communicate with the backend servers.
protection_status	No	String	Definition: Specifies the protection status. Constraints: N/A Range: • nonProtection (default): The resource is not protected. • consoleProtection: Modifications are not allowed on the console. Default value: N/A

Parameter	Mandatory	Type	Description
protection_reason	No	String	Definition: Specifies why modification protection is enabled. Constraints: This parameter is valid only when protection_status is set to consoleProtection . Range: The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>). Default value: N/A
gzip_enable	No	Boolean	Definition: Specifies whether to enable gzip_enable for a load balancer. Constraints: This parameter can be configured only for HTTP, HTTPS, and QUIC listeners. Range: The value can be true (enable this option) or false (disable this option). Default value: false
port_ranges	No	Array of PortRange objects	Definition: Specifies one or more port ranges, including the start and end port numbers. A maximum of 10 port ranges can be specified. Port ranges cannot overlap with each other. Constraints: • 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	Definition: Specifies whether to enable zero round trip time resumption (0-RTT) for listeners. Constraints: 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 , there may be replay attacks. Range: true or false Default value: false
cps	No	Integer	Definition: Specifies the maximum number of new connections that a listener can handle per second. Constraints: If the value is greater than the number defined in the load balancer flavors, the latter is used as the limit. Range: 0 to 1000000 Default value: 0 , indicating that the number is not limited.
connection	No	Integer	Definition: Specifies the maximum number of concurrent connections that a listener can handle per second. Constraints: If the value is greater than the number defined in the load balancer flavors, the latter is used as the limit. Range: 0 to 1000000 Default value: 0 , indicating that the number is not limited.

Parameter	Mandatory	Type	Description
nat64_enable	No	Boolean	Definition: Specifies whether to translate between IPv4 and IPv6 addresses. This option allows 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 . Range: true: Enable nat64_enable . false: Disable nat64_enable . Default value: false

Table 5-314 ListenerInsertHeaders

Parameter	Mandatory	Type	Description
X-Forwarded-ELB-IP	No	Boolean	Definition: If X-Forwarded-ELB-IP is set to true , the load balancer EIP will be stored in the X-Forwarded-ELB-IP header and passed to backend servers. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-Port	No	Boolean	Definition: If X-Forwarded-Port is set to true , the listening port of the load balancer will be stored in the X-Forwarded-Port header and passed to backend servers. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
X-Forwarded-For-Port	No	Boolean	Definition: 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. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-Host	No	Boolean	Definition: If X-Forwarded-Host is set to true , the client host can be stored in the X-Forwarded-Host header and passed to backend servers. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-Proto	No	Boolean	Definition: If X-Forwarded-Proto is set to true , the listener protocol of the load balancer can be stored in the X-Forwarded-Proto header and passed to backend servers. Constraints: N/A Range: N/A Default value: N/A
X-Real-IP	No	Boolean	Definition: If X-Real-IP is set to true , the client IP address can be stored in the X-Real-IP header and passed to backend servers. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
X-Forwarded-ELB-ID	No	Boolean	Definition: If X-Forwarded-ELB-ID is set to true , the load balancer ID can be transferred to backend servers through the X-Forwarded-ELB-ID header. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-TLS-Certificate-ID	No	Boolean	Definition: 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 X-Forwarded-TLS-Certificate-ID header. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-TLS-Protocol	No	Boolean	Definition: If X-Forwarded-TLS-Protocol is set to true , the algorithm protocol of the load balancer can be transferred to backend servers through the X-Forwarded-TLS-Protocol header. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-TLS-Cipher	No	Boolean	Definition: If X-Forwarded-TLS-Cipher is set to true , the algorithm suite of the load balancer can be transferred to backend servers through the X-Forwarded-TLS-Cipher header. Constraints: N/A Range: N/A Default value: N/A

Table 5-315 Tag

Parameter	Mandatory	Type	Description
key	No	String	Definition: Specifies the tag key. Range: N/A
value	No	String	Definition: Specifies the tag value. Range: N/A

Table 5-316 CreateListenerIpGroupOption

Parameter	Mandatory	Type	Description
ipgroup_id	Yes	String	Definition: Specifies the ID of the IP address group associated with the listener. Constraints: - 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. Range: N/A Default value: N/A
enable_ipgroup	No	Boolean	Definition: Specifies whether to enable access control. Constraints: N/A Range: true (default): Enable access control. false: Disable access control. Default value: N/A

Parameter	Mandatory	Type	Description
type	No	String	Definition: Specifies how access to the listener is controlled. Constraints: N/A Range: • white: 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. Default value: white

Table 5-317 CreateListenerQuicConfigOption

Parameter	Mandatory	Type	Description
quic_listener_id	Yes	String	Definition: Specifies the ID of the QUIC listener. Constraints: 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 . Range: N/A Default value: N/A
enable_quic_upgrade	No	Boolean	Definition: Specifies whether to enable QUIC upgrade. If this option is enabled, HTTPS listeners will be upgraded to QUIC listeners. Constraints: N/A Range: • True: Enable QUIC upgrade. • False: Disable QUIC upgrade. Default value: false

Table 5-318 PortRange

Parameter	Mandatory	Type	Description
start_port	No	Integer	Definition: Specifies the start port number. Constraints: N/A Range: 1-65535 Default value: N/A
end_port	No	Integer	Definition: Specifies the end port number. The value must be greater than or equal to the start port number. Constraints: N/A Range: 1-65535 Default value: N/A

Response Parameters

Status code: 201

Table 5-319 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
listener	Listener object	Definition: Specifies the listener.

Table 5-320 Listener

Parameter	Type	Description
admin_state_up	Boolean	Definition: Specifies the administrative status of the listener. Default value: true
client_ca_tls_container_ref	String	Definition: Specifies the ID of the CA certificate used by the listener. This parameter is available only when type is set to client . Default value: N/A

Parameter	Type	Description
connection_limit	Integer	Definition: Specifies the maximum number of connections that the listener can establish with backend servers. Range: an integer greater than or equal to -1
created_at	String	Definition: Specifies the time when the listener was created. Range: N/A The value must be in the format of <i>yyyy-MM-dd"T"HH:mm:ss"Z"</i> , for example, 2021-07-30T12:03:44Z.
default_pool_id	String	Definition: Specifies the ID of the default backend server group of the listener. If there is no matched forwarding policy, requests will be routed to the default backend server group. Range: N/A
default_tls_container_ref	String	Definition: Specifies the ID of the server certificate used by the listener. Default value: N/A
description	String	Definition: Provides supplementary information about the listener. Range: N/A
http2_enable	Boolean	Definition: Specifies whether to allow clients to use HTTP/2 to communicate with the load balancer for higher access performance. However, the load balancer still uses HTTP/1.x to forward requests to the backend server. Range: N/A
id	String	Definition: Specifies the listener ID. Range: N/A
insert_headers	ListenerInsertHeaders object	Definition: Specifies the HTTP headers that can transmit required information to backend servers. For example, you can use the X-Forwarded-ELB-IP header to transmit the load balancer EIP to backend servers.

Parameter	Type	Description
loadbalancers	Array of LoadBalancerRef objects	Definition: Specifies the ID of the load balancer that the listener is added to. A listener can be associated with only one load balancer.
name	String	Definition: Specifies the name of the listener. If you leave the listener name empty, you cannot locate it in the listener list and view its details. Range: N/A
project_id	String	Definition: Specifies the ID of the project that the listener belongs to. Range: N/A
enterprise_project_id	String	Definition: Specifies the enterprise project ID. Range: N/A
protocol	String	Definition: Specifies the protocol of the listener. Range: TCP, UDP, HTTP, HTTPS, TERMINATED_HTTPS, QUIC, or TLS.
protocol_port	Integer	Definition: Specifies the port used by the listener. Default value: N/A
sni_container_refs	Array of strings	Definition: Specifies the IDs of SNI certificates (server certificates with domain names) used by the listener. Range: N/A
sni_match_algo	String	Definition: Specifies how wildcard domain name matches with the SNI certificates used by the listener. Range: longest_suffix indicates longest suffix match. wildcard indicates wildcard match.
tags	Array of Tag objects	Definition: Lists the tags.
updated_at	String	Definition: Specifies the time when the listener was updated. Range: The value must be in the format of <i>yyyy-MM-dd"T"HH:mm:ss"Z"</i> , for example, 2021-07-30T12:03:44Z.

Parameter	Type	Description
tls_ciphers_policy	String	Definition: Specifies the security policy used by the listener. Range: tls-1-0-inherit, tls-1-0, tls-1-1, tls-1-2, 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. The default value is tls-1-2.
security_policy_id	String	Definition: Specifies the ID of the custom security policy. Range: N/A
enable_member_retry	Boolean	Definition: Specifies whether to enable health check retries for backend servers. Range: true indicates health check retries will be enabled. false indicates health check retries will be disabled.
keepalive_timeout	Integer	Definition: Specifies the idle timeout duration, in seconds. If the load balancer receives no requests within the idle timeout duration, it will disconnect the connection with the client and establish a new connection when there is a new request. Range: - For TCP listeners, the value ranges from 10s to 4000s. - For HTTP, HTTPS, and TERMINATED_HTTPS listeners, the value ranges from 0s to 4000s.
client_timeout	Integer	Definition: 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. Range: 1-300

Parameter	Type	Description
member_timeout	Integer	Definition: 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. Range: 1-300
ipgroup	ListenerIpGroup object	Definition: Specifies the IP address group associated with the listener.
transparent_client_ip_enable	Boolean	Definition: Specifies whether to pass source IP addresses of the clients to backend servers. If it is enabled, the source IP addresses of the clients will be passed to the backend server. This parameter applies only to TCP/UDP listeners added to a shared load balancer. Range: • 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.
proxy_protocol_enable	Boolean	Definition: Specifies whether to enable ProxyProtocol 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. Range: The value can be true (enable this option) or false (disable this option).

Parameter	Type	Description
enhance_l7policy_enable	Boolean	Definition: Specifies whether to enable advanced forwarding. If advanced forwarding is enabled, more flexible forwarding policies and rules are supported. 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. Range: The value can be true (enable this option) or false (disable this option).
quic_config	ListenerQuicConfig object	Definition: Specifies the QUIC configuration for the current listener.
protection_status	String	Definition: Specifies the protection status. Range: • nonProtection: The resource is not protected. • consoleProtection: Modification is not allowed on the console.
protection_reason	String	Definition: Specifies why modification protection is enabled. Range: The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).

Parameter	Type	Description
gzip_enable	Boolean	Definition: Specifies whether to enable gzip_enable for a load balancer. Range: The value can be true (enable this option) or false (disable this option).
port_ranges	Array of PortRange objects	Definition: Specifies one or more port ranges, including the start and end ports.
ssl_early_data_enable	Boolean	Definition: Specifies whether to enable zero round trip time resumption (0-RTT) for listeners. Constraints: This option can be configured only for HTTPS listeners and depends on the TLS 1.3 security policy protocols.
cps	Integer	Definition: Specifies the maximum number of new connections that a listener can handle per second. If the value is greater than the number defined in the load balancer flavors, the latter is used as the limit. Range: 0 to 1000000
connection	Integer	Definition: Specifies the maximum number of concurrent connections that a listener can handle per second. If the value is greater than the number defined in the load balancer flavors, the latter is used as the limit. Range: 0 to 1000000
nat64_enable	Boolean	Definition: Specifies whether to translate between IPv4 and IPv6 addresses. This option allows a client to access IPv4 or IPv6 backend servers by accessing the IPv4 or IPv6 address of a load balancer. Range: true: Enable nat64_enable . false: Disable nat64_enable .

Table 5-321 ListenerInsertHeaders

Parameter	Type	Description
X-Forwarded-ELB-IP	Boolean	Definition: If X-Forwarded-ELB-IP is set to true , the load balancer EIP will be stored in the X-Forwarded-ELB-IP header and passed to backend servers. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-Port	Boolean	Definition: If X-Forwarded-Port is set to true , the listening port of the load balancer will be stored in the X-Forwarded-Port header and passed to backend servers. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-For-Port	Boolean	Definition: 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. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-Host	Boolean	Definition: If X-Forwarded-Host is set to true , the client host can be stored in the X-Forwarded-Host header and passed to backend servers. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-Proto	Boolean	Definition: If X-Forwarded-Proto is set to true , the listener protocol of the load balancer can be stored in the X-Forwarded-Proto header and passed to backend servers. Constraints: N/A Range: N/A Default value: N/A

Parameter	Type	Description
X-Real-IP	Boolean	Definition: If X-Real-IP is set to true , the client IP address can be stored in the X-Real-IP header and passed to backend servers. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-ELB-ID	Boolean	Definition: If X-Forwarded-ELB-ID is set to true , the load balancer ID can be transferred to backend servers through the X-Forwarded-ELB-ID header. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-TLS-Certificate-ID	Boolean	Definition: 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 X-Forwarded-TLS-Certificate-ID header. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-TLS-Protocol	Boolean	Definition: If X-Forwarded-TLS-Protocol is set to true , the algorithm protocol of the load balancer can be transferred to backend servers through the X-Forwarded-TLS-Protocol header. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-TLS-Cipher	Boolean	Definition: If X-Forwarded-TLS-Cipher is set to true , the algorithm suite of the load balancer can be transferred to backend servers through the X-Forwarded-TLS-Cipher header. Constraints: N/A Range: N/A Default value: N/A

Table 5-322 LoadBalancerRef

Parameter	Type	Description
id	String	Definition: Specifies the load balancer ID. Range: N/A

Table 5-323 Tag

Parameter	Type	Description
key	String	Definition: Specifies the tag key. Range: N/A
value	String	Definition: Specifies the tag value. Range: N/A

Table 5-324 ListenerIpGroup

Parameter	Type	Description
ipgroup_id	String	Definition: Specifies the ID of the IP address group associated with the listener. This parameter is mandatory during creation and is optional during update. Constraints: The specified IP address group must exist, and the value cannot be null . Otherwise, the IP address group conflicts with enable_ipgroup .
enable_ipgroup	Boolean	Definition: Specifies whether access control is enabled. A listener with access control enabled can be directly deleted. Range: • true: Access control is enabled. • false: Access control is disabled.

Parameter	Type	Description
type	String	Definition: Specifies how access to the listener is controlled. Range: • white: 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 5-325 ListenerQuicConfig

Parameter	Type	Description
quic_listener_id	String	Definition: Specifies the ID of the QUIC listener. Range: N/A
enable_quic_upgrade	Boolean	Definition: Specifies whether to enable QUIC upgrade. If this option is enabled, HTTPS listeners will be upgraded to QUIC listeners. Range: • True: Enable QUIC upgrade. • False: Disable QUIC upgrade.

Table 5-326 PortRange

Parameter	Type	Description
start_port	Integer	Definition: Specifies the start port number. Constraints: N/A Range: 1-65535 Default value: N/A
end_port	Integer	Definition: Specifies the end port number. The value must be greater than or equal to the start port number. Constraints: N/A Range: 1-65535 Default value: N/A

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

Successful request.

```
{
  "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 huaweicloudskelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskelb.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.ElClientBuilder().
        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{}
typelpgroup:= model.GetCreateListenerIpGroupOptionTypeEnum().BLACK
ipgroupListener := &model.CreateListenerIpGroupOption{
    IpgroupId: "0416b6f1-877f-4a51-987e-978b3f083542",
    Type: &typelpgroup,
}
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	Successful request.

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 5-327 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Table 5-328 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Definition: Specifies the number of records returned on each page. Constraints: N/A Range: 0 to 2000 Default value: 2000

Parameter	Mandatory	Type	Description
marker	No	String	Definition: Specifies the ID of the last record on the previous page. Constraints: • This parameter must be used together with limit. • If the parameter is not specified, only resources on the first page are queried. • This parameter cannot be left blank or set to an invalid ID. Range: N/A Default value: N/A
page_reverse	No	Boolean	Definition: Specifies whether to use reverse query. Constraints: • This parameter must be used together with limit. • If page_reverse is set to true and you want to query the resources on the previous page, set the value of marker to the value of previous_marker. Range: • true: Query resources on the previous page. • false: Query resources on the next page. Default value: false
protocol_port	No	Array of strings	Definition: Specifies the port used by the listener. Multiple ports can be used for query in the format of <i>protocol_port=xxx&protocol_port=xxx</i> . Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
protocol	No	Array of strings	Definition: Specifies the protocol used by the listener. Multiple protocols can be used for query in the format of <i>protocol=xxx&protocol=xxx</i> . Constraints: N/A The value can be TCP, UDP, HTTP, HTTPS, TERMINATED_HTTPS, QUIC, or TLS . Default value: N/A
description	No	Array of strings	Definition: Provides supplementary information about the listener. Multiple descriptions can be used for query in the format of <i>description=xxx&description=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
default_tls_container_ref	No	Array of strings	Definition: Specifies the ID of the server certificate used by the listener. Multiple IDs can be used for query in the format of <i>default_tls_container_ref=xxx&default_tls_container_ref=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
client_ca_tls_container_ref	No	Array of strings	Definition: Specifies the ID of the CA certificate used by the listener. Multiple IDs can be used for query in the format of <i>client_ca_tls_container_ref=xxx&client_ca_tls_container_ref=xxx</i> . Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Definition: Specifies the administrative status of the listener. Constraints: N/A Range: N/A Default value: N/A
include_recycle_bin	No	Boolean	Definition: Specifies whether to query the listeners associated with the load balancers in the recycle bin. Constraints: N/A Range: • true: Listeners associated with the load balancers in the recycle bin are returned. • false: Listeners associated with the load balancers in the recycle bin are not returned. Default value: N/A
connection_limit	No	Array of integers	Definition: Specifies the maximum number of connections that the load balancer can establish with backend servers. Multiple values can be used for query in the format of <i>connection_limit=xxx&connection_limit=xxx</i> . Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
default_pool_id	No	Array of strings	Definition: 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 group. Multiple IDs can be used for query in the format of <i>default_pool_id=xxx&default_pool_id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
id	No	Array of strings	Definition: Specifies the listener ID. Multiple IDs can be used for query in the format of <i>id=xxx&id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
name	No	Array of strings	Definition: Specifies the name of the listener added to the load balancer. Multiple names can be used for query in the format of <i>name=xxx&name=xxx</i> . Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
http2_enable	No	Boolean	Definition: 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. Constraints: N/A Range: The value can be true (enable this option) or false (disable this option). Default value: N/A
loadbalancer_id	No	Array of strings	Definition: Specifies the ID of the load balancer that the listener is added to. Multiple IDs can be used for query in the format of <i>loadbalancer_id=xxx&loadbalancer_id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
tls_ciphers_policy	No	Array of strings	Definition: Specifies the security policy used by the listener. Multiple security policies can be used for query in the format of <i>tls_ciphers_policy=xxx&tls_ciphers_policy=xxx</i> . Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
member_address	No	Array of strings	Definition: Specifies the IP address of the backend server. This is a query parameter and will not be included in the response. Multiple IP addresses can be used for query in the format of <i>member_address=xxx&member_address=xxx.</i> Constraints: N/A Range: N/A Default value: N/A
member_device_id	No	Array of strings	Definition: Specifies the ID of the ECS 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 used for query in the format of <i>member_device_id=xxx&member_device_id=xxx.</i> Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
enterprise_project_id	No	Array of strings	Definition: Specifies the ID of the enterprise project. Multiple values can be used for query in the format of: <i>enterprise_project_id=xxx&enterprise_project_id=xxx.</i> Constraints: • 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. Range: N/A Default value: N/A
enable_member_retry	No	Boolean	Definition: Specifies whether to enable health check retries for backend servers. Constraints: N/A Range: The value can be true (enable health check retries) or false (disable health check retries). Default value: N/A

Parameter	Mandatory	Type	Description
member_timeout	No	Array of integers	Definition: 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. Multiple durations can be used for query in the format of <i>member_timeout=xxx&member_timeout=xxx.</i> Constraints: N/A Range: N/A Default value: N/A
client_timeout	No	Array of integers	Definition: 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. Multiple durations can be used for query in the format of <i>client_timeout=xxx&client_timeout=xxx.</i> Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
keepalive_timeout	No	Array of integers	Definition: Specifies the idle timeout duration, in seconds. If the load balancer receives no requests within the idle timeout duration, it will disconnect the connection with the client and establish a new connection when there is a new request. Multiple durations can be used for query in the format of <i>keepalive_timeout=xxx&keepalive_timeout=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
transparent_client_ip_enable	No	Boolean	Definition: 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. Constraints: N/A Range: The value can be true (enable this option) or false (disable this option). Default value: N/A
proxy_protocol_enable	No	Boolean	Definition: Specifies whether to enable the ProxyProtocol option to pass the source IP addresses of the clients to backend servers. Constraints: N/A Range: The value can be true (enable this option) or false (disable this option). Default value: N/A

Parameter	Mandatory	Type	Description
enhance_l7policy_enable	No	Boolean	Definition: Specifies whether to enable advanced forwarding. If you enable this function, you can configure more flexible forwarding policies and rules. Constraints: N/A Range: The value can be true (enable this option) or false (disable this option). Default value: N/A
member_instance_id	No	Array of strings	Definition: Specifies the backend server ID. This is a query parameter and will not be included in the response. Multiple IDs can be used for query in the format of <i>member_instance_id=xxx&member_instance_id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
protection_status	No	Array of strings	Definition: Specifies the protection status. Multiple statuses can be used for query in the format of <i>protection_status=xxx&protection_status=xxx</i> . Constraints: N/A Range: • nonProtection: The resource is not protected. • consoleProtection: Modification is not allowed on the console. Default value: nonProtection

Parameter	Mandatory	Type	Description
ssl_early_data_enable	No	Boolean	Definition: Specifies whether to enable zero round trip time resumption (0-RTT) for listeners. Constraints: N/A Range: The value can be true (enable this option) or false (disable this option). Default value: N/A
nat64_enable	No	Boolean	Definition: Specifies whether to set nat64_enable to true . Constraints: N/A Range: The value can be true (enable this option) or false (disable this option). Default value: N/A

Request Parameters

Table 5-329 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-330 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

Parameter	Type	Description
page_info	PageInfo object	Definition: Specifies the pagination information.
listeners	Array of Listener objects	Definition: Lists the listeners.

Table 5-331 PageInfo

Parameter	Type	Description
previous_marker	String	Definition: Specifies the ID of the first record in the pagination query result. If page_reverse is set to true , this parameter is used together to query resources on the previous page. Range: N/A
next_marker	String	Definition: Specifies the ID of the last record in the pagination query result. It is usually used to query resources on the next page. Range: N/A
current_count	Integer	Definition: Specifies the number of records returned on the current page. Range: N/A

Table 5-332 Listener

Parameter	Type	Description
admin_state_up	Boolean	Definition: Specifies the administrative status of the listener. Default value: true
client_ca_tls_container_ref	String	Definition: Specifies the ID of the CA certificate used by the listener. This parameter is available only when type is set to client . Default value: N/A
connection_limit	Integer	Definition: Specifies the maximum number of connections that the listener can establish with backend servers. Range: an integer greater than or equal to -1

Parameter	Type	Description
created_at	String	Definition: Specifies the time when the listener was created. Range: N/A The value must be in the format of <i>yyyy-MM-dd"T"HH:mm:ss"Z"</i> , for example, 2021-07-30T12:03:44Z.
default_pool_id	String	Definition: Specifies the ID of the default backend server group of the listener. If there is no matched forwarding policy, requests will be routed to the default backend server group. Range: N/A
default_tls_container_ref	String	Definition: Specifies the ID of the server certificate used by the listener. Default value: N/A
description	String	Definition: Provides supplementary information about the listener. Range: N/A
http2_enable	Boolean	Definition: Specifies whether to allow clients to use HTTP/2 to communicate with the load balancer for higher access performance. However, the load balancer still uses HTTP/1.x to forward requests to the backend server. Range: N/A
id	String	Definition: Specifies the listener ID. Range: N/A
insert_headers	ListenerInsertHeaders object	Definition: Specifies the HTTP headers that can transmit required information to backend servers. For example, you can use the X-Forwarded-ELB-IP header to transmit the load balancer EIP to backend servers.
loadbalancers	Array of LoadBalancerRef objects	Definition: Specifies the ID of the load balancer that the listener is added to. A listener can be associated with only one load balancer.

Parameter	Type	Description
name	String	Definition: Specifies the name of the listener. If you leave the listener name empty, you cannot locate it in the listener list and view its details. Range: N/A
project_id	String	Definition: Specifies the ID of the project that the listener belongs to. Range: N/A
enterprise_project_id	String	Definition: Specifies the enterprise project ID. Range: N/A
protocol	String	Definition: Specifies the protocol of the listener. Range: TCP, UDP, HTTP, HTTPS, TERMINATED_HTTPS, QUIC, or TLS.
protocol_port	Integer	Definition: Specifies the port used by the listener. Default value: N/A
sni_container_refs	Array of strings	Definition: Specifies the IDs of SNI certificates (server certificates with domain names) used by the listener. Range: N/A
sni_match_algo	String	Definition: Specifies how wildcard domain name matches with the SNI certificates used by the listener. Range: longest_suffix indicates longest suffix match. wildcard indicates wildcard match.
tags	Array of Tag objects	Definition: Lists the tags.
updated_at	String	Definition: Specifies the time when the listener was updated. Range: The value must be in the format of <i>yyyy-MM-dd"T"HH:mm:ss"Z"</i> , for example, 2021-07-30T12:03:44Z.

Parameter	Type	Description
tls_ciphers_policy	String	Definition: Specifies the security policy used by the listener. Range: tls-1-0-inherit, tls-1-0, tls-1-1, tls-1-2, 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. The default value is tls-1-2.
security_policy_id	String	Definition: Specifies the ID of the custom security policy. Range: N/A
enable_member_retry	Boolean	Definition: Specifies whether to enable health check retries for backend servers. Range: true indicates health check retries will be enabled. false indicates health check retries will be disabled.
keepalive_timeout	Integer	Definition: Specifies the idle timeout duration, in seconds. If the load balancer receives no requests within the idle timeout duration, it will disconnect the connection with the client and establish a new connection when there is a new request. Range: - For TCP listeners, the value ranges from 10s to 4000s. - For HTTP, HTTPS, and TERMINATED_HTTPS listeners, the value ranges from 0s to 4000s.
client_timeout	Integer	Definition: 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. Range: 1-300

Parameter	Type	Description
member_timeout	Integer	Definition: 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. Range: 1-300
ipgroup	ListenerIpGroup object	Definition: Specifies the IP address group associated with the listener.
transparent_client_ip_enable	Boolean	Definition: Specifies whether to pass source IP addresses of the clients to backend servers. If it is enabled, the source IP addresses of the clients will be passed to the backend server. This parameter applies only to TCP/UDP listeners added to a shared load balancer. Range: • 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.
proxy_protocol_enable	Boolean	Definition: Specifies whether to enable ProxyProtocol 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. Range: The value can be true (enable this option) or false (disable this option).

Parameter	Type	Description
enhance_l7policy_enable	Boolean	Definition: Specifies whether to enable advanced forwarding. If advanced forwarding is enabled, more flexible forwarding policies and rules are supported. 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. Range: The value can be true (enable this option) or false (disable this option).
quic_config	ListenerQuicConfig object	Definition: Specifies the QUIC configuration for the current listener.
protection_status	String	Definition: Specifies the protection status. Range: • nonProtection: The resource is not protected. • consoleProtection: Modification is not allowed on the console.
protection_reason	String	Definition: Specifies why modification protection is enabled. Range: The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).

Parameter	Type	Description
gzip_enable	Boolean	Definition: Specifies whether to enable gzip_enable for a load balancer. Range: The value can be true (enable this option) or false (disable this option).
port_ranges	Array of PortRange objects	Definition: Specifies one or more port ranges, including the start and end ports.
ssl_early_data_enable	Boolean	Definition: Specifies whether to enable zero round trip time resumption (0-RTT) for listeners. Constraints: This option can be configured only for HTTPS listeners and depends on the TLS 1.3 security policy protocols.
cps	Integer	Definition: Specifies the maximum number of new connections that a listener can handle per second. If the value is greater than the number defined in the load balancer flavors, the latter is used as the limit. Range: 0 to 1000000
connection	Integer	Definition: Specifies the maximum number of concurrent connections that a listener can handle per second. If the value is greater than the number defined in the load balancer flavors, the latter is used as the limit. Range: 0 to 1000000
nat64_enable	Boolean	Definition: Specifies whether to translate between IPv4 and IPv6 addresses. This option allows a client to access IPv4 or IPv6 backend servers by accessing the IPv4 or IPv6 address of a load balancer. Range: true: Enable nat64_enable . false: Disable nat64_enable .

Table 5-333 ListenerInsertHeaders

Parameter	Type	Description
X-Forwarded-ELB-IP	Boolean	Definition: If X-Forwarded-ELB-IP is set to true , the load balancer EIP will be stored in the X-Forwarded-ELB-IP header and passed to backend servers. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-Port	Boolean	Definition: If X-Forwarded-Port is set to true , the listening port of the load balancer will be stored in the X-Forwarded-Port header and passed to backend servers. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-For-Port	Boolean	Definition: 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. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-Host	Boolean	Definition: If X-Forwarded-Host is set to true , the client host can be stored in the X-Forwarded-Host header and passed to backend servers. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-Proto	Boolean	Definition: If X-Forwarded-Proto is set to true , the listener protocol of the load balancer can be stored in the X-Forwarded-Proto header and passed to backend servers. Constraints: N/A Range: N/A Default value: N/A

Parameter	Type	Description
X-Real-IP	Boolean	Definition: If X-Real-IP is set to true , the client IP address can be stored in the X-Real-IP header and passed to backend servers. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-ELB-ID	Boolean	Definition: If X-Forwarded-ELB-ID is set to true , the load balancer ID can be transferred to backend servers through the X-Forwarded-ELB-ID header. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-TLS-Certificate-ID	Boolean	Definition: 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 X-Forwarded-TLS-Certificate-ID header. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-TLS-Protocol	Boolean	Definition: If X-Forwarded-TLS-Protocol is set to true , the algorithm protocol of the load balancer can be transferred to backend servers through the X-Forwarded-TLS-Protocol header. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-TLS-Cipher	Boolean	Definition: If X-Forwarded-TLS-Cipher is set to true , the algorithm suite of the load balancer can be transferred to backend servers through the X-Forwarded-TLS-Cipher header. Constraints: N/A Range: N/A Default value: N/A

Table 5-334 LoadBalancerRef

Parameter	Type	Description
id	String	Definition: Specifies the load balancer ID. Range: N/A

Table 5-335 Tag

Parameter	Type	Description
key	String	Definition: Specifies the tag key. Range: N/A
value	String	Definition: Specifies the tag value. Range: N/A

Table 5-336 ListenerIpGroup

Parameter	Type	Description
ipgroup_id	String	Definition: Specifies the ID of the IP address group associated with the listener. This parameter is mandatory during creation and is optional during update. Constraints: The specified IP address group must exist, and the value cannot be null . Otherwise, the IP address group conflicts with enable_ipgroup .
enable_ipgroup	Boolean	Definition: Specifies whether access control is enabled. A listener with access control enabled can be directly deleted. Range: • true: Access control is enabled. • false: Access control is disabled.

Parameter	Type	Description
type	String	Definition: Specifies how access to the listener is controlled. Range: • white: 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 5-337 ListenerQuicConfig

Parameter	Type	Description
quic_listener_id	String	Definition: Specifies the ID of the QUIC listener. Range: N/A
enable_quic_upgrade	Boolean	Definition: Specifies whether to enable QUIC upgrade. If this option is enabled, HTTPS listeners will be upgraded to QUIC listeners. Range: • True: Enable QUIC upgrade. • False: Disable QUIC upgrade.

Table 5-338 PortRange

Parameter	Type	Description
start_port	Integer	Definition: Specifies the start port number. Constraints: N/A Range: 1-65535 Default value: N/A
end_port	Integer	Definition: Specifies the end port number. The value must be greater than or equal to the start port number. Constraints: N/A Range: 1-65535 Default value: N/A

Example Requests

Querying 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 5-339 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
listener_id	Yes	String	Definition: Specifies the listener ID. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-340 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-341 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

Parameter	Type	Description
listener	Listener object	Definition: Specifies the listener.

Table 5-342 Listener

Parameter	Type	Description
admin_state_up	Boolean	Definition: Specifies the administrative status of the listener. Default value: true
client_ca_tls_container_ref	String	Definition: Specifies the ID of the CA certificate used by the listener. This parameter is available only when type is set to client . Default value: N/A
connection_limit	Integer	Definition: Specifies the maximum number of connections that the listener can establish with backend servers. Range: an integer greater than or equal to -1
created_at	String	Definition: Specifies the time when the listener was created. Range: N/A The value must be in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> , for example, 2021-07-30T12:03:44Z.
default_pool_id	String	Definition: Specifies the ID of the default backend server group of the listener. If there is no matched forwarding policy, requests will be routed to the default backend server group. Range: N/A
default_tls_container_ref	String	Definition: Specifies the ID of the server certificate used by the listener. Default value: N/A
description	String	Definition: Provides supplementary information about the listener. Range: N/A

Parameter	Type	Description
http2_enable	Boolean	Definition: Specifies whether to allow clients to use HTTP/2 to communicate with the load balancer for higher access performance. However, the load balancer still uses HTTP/1.x to forward requests to the backend server. Range: N/A
id	String	Definition: Specifies the listener ID. Range: N/A
insert_headers	ListenerInsertHeaders object	Definition: Specifies the HTTP headers that can transmit required information to backend servers. For example, you can use the X-Forwarded-ELB-IP header to transmit the load balancer EIP to backend servers.
loadbalancers	Array of LoadBalancerRef objects	Definition: Specifies the ID of the load balancer that the listener is added to. A listener can be associated with only one load balancer.
name	String	Definition: Specifies the name of the listener. If you leave the listener name empty, you cannot locate it in the listener list and view its details. Range: N/A
project_id	String	Definition: Specifies the ID of the project that the listener belongs to. Range: N/A
enterprise_project_id	String	Definition: Specifies the enterprise project ID. Range: N/A
protocol	String	Definition: Specifies the protocol of the listener. Range: TCP, UDP, HTTP, HTTPS, TERMINATED_HTTPS, QUIC, or TLS.
protocol_port	Integer	Definition: Specifies the port used by the listener. Default value: N/A

Parameter	Type	Description
sni_container_refs	Array of strings	Definition: Specifies the IDs of SNI certificates (server certificates with domain names) used by the listener. Range: N/A
sni_match_algo	String	Definition: Specifies how wildcard domain name matches with the SNI certificates used by the listener. Range: longest_suffix indicates longest suffix match. wildcard indicates wildcard match.
tags	Array of Tag objects	Definition: Lists the tags.
updated_at	String	Definition: Specifies the time when the listener was updated. Range: The value must be in the format of <i>yyyy-MM-dd"T"HH:mm:ss"Z"</i> , for example, 2021-07-30T12:03:44Z.
tls_ciphers_policy	String	Definition: Specifies the security policy used by the listener. Range: tls-1-0-inherit, tls-1-0, tls-1-1, tls-1-2, 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. The default value is tls-1-2.
security_policy_id	String	Definition: Specifies the ID of the custom security policy. Range: N/A
enable_member_retry	Boolean	Definition: Specifies whether to enable health check retries for backend servers. Range: true indicates health check retries will be enabled. false indicates health check retries will be disabled.

Parameter	Type	Description
keepalive_timeout	Integer	Definition: Specifies the idle timeout duration, in seconds. If the load balancer receives no requests within the idle timeout duration, it will disconnect the connection with the client and establish a new connection when there is a new request. Range: - For TCP listeners, the value ranges from 10s to 4000s. - For HTTP, HTTPS, and TERMINATED_HTTPS listeners, the value ranges from 0s to 4000s.
client_timeout	Integer	Definition: 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. Range: 1-300
member_timeout	Integer	Definition: 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. Range: 1-300
ipgroup	ListenerIpGroup object	Definition: Specifies the IP address group associated with the listener.

Parameter	Type	Description
transparent_client_ip_enable	Boolean	Definition: Specifies whether to pass source IP addresses of the clients to backend servers. If it is enabled, the source IP addresses of the clients will be passed to the backend server. This parameter applies only to TCP/UDP listeners added to a shared load balancer. Range: • 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.
proxy_protocol_enable	Boolean	Definition: Specifies whether to enable ProxyProtocol 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. Range: The value can be true (enable this option) or false (disable this option).

Parameter	Type	Description
enhance_l7policy_enable	Boolean	Definition: Specifies whether to enable advanced forwarding. If advanced forwarding is enabled, more flexible forwarding policies and rules are supported. 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. Range: The value can be true (enable this option) or false (disable this option).
quic_config	ListenerQuicConfig object	Definition: Specifies the QUIC configuration for the current listener.
protection_status	String	Definition: Specifies the protection status. Range: • nonProtection: The resource is not protected. • consoleProtection: Modification is not allowed on the console.
protection_reason	String	Definition: Specifies why modification protection is enabled. Range: The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).

Parameter	Type	Description
gzip_enable	Boolean	Definition: Specifies whether to enable gzip_enable for a load balancer. Range: The value can be true (enable this option) or false (disable this option).
port_ranges	Array of PortRange objects	Definition: Specifies one or more port ranges, including the start and end ports.
ssl_early_data_enable	Boolean	Definition: Specifies whether to enable zero round trip time resumption (0-RTT) for listeners. Constraints: This option can be configured only for HTTPS listeners and depends on the TLS 1.3 security policy protocols.
cps	Integer	Definition: Specifies the maximum number of new connections that a listener can handle per second. If the value is greater than the number defined in the load balancer flavors, the latter is used as the limit. Range: 0 to 1000000
connection	Integer	Definition: Specifies the maximum number of concurrent connections that a listener can handle per second. If the value is greater than the number defined in the load balancer flavors, the latter is used as the limit. Range: 0 to 1000000
nat64_enable	Boolean	Definition: Specifies whether to translate between IPv4 and IPv6 addresses. This option allows a client to access IPv4 or IPv6 backend servers by accessing the IPv4 or IPv6 address of a load balancer. Range: true: Enable nat64_enable . false: Disable nat64_enable .

Table 5-343 ListenerInsertHeaders

Parameter	Type	Description
X-Forwarded-ELB-IP	Boolean	Definition: If X-Forwarded-ELB-IP is set to true , the load balancer EIP will be stored in the X-Forwarded-ELB-IP header and passed to backend servers. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-Port	Boolean	Definition: If X-Forwarded-Port is set to true , the listening port of the load balancer will be stored in the X-Forwarded-Port header and passed to backend servers. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-For-Port	Boolean	Definition: 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. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-Host	Boolean	Definition: If X-Forwarded-Host is set to true , the client host can be stored in the X-Forwarded-Host header and passed to backend servers. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-Proto	Boolean	Definition: If X-Forwarded-Proto is set to true , the listener protocol of the load balancer can be stored in the X-Forwarded-Proto header and passed to backend servers. Constraints: N/A Range: N/A Default value: N/A

Parameter	Type	Description
X-Real-IP	Boolean	Definition: If X-Real-IP is set to true , the client IP address can be stored in the X-Real-IP header and passed to backend servers. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-ELB-ID	Boolean	Definition: If X-Forwarded-ELB-ID is set to true , the load balancer ID can be transferred to backend servers through the X-Forwarded-ELB-ID header. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-TLS-Certificate-ID	Boolean	Definition: 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 X-Forwarded-TLS-Certificate-ID header. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-TLS-Protocol	Boolean	Definition: If X-Forwarded-TLS-Protocol is set to true , the algorithm protocol of the load balancer can be transferred to backend servers through the X-Forwarded-TLS-Protocol header. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-TLS-Cipher	Boolean	Definition: If X-Forwarded-TLS-Cipher is set to true , the algorithm suite of the load balancer can be transferred to backend servers through the X-Forwarded-TLS-Cipher header. Constraints: N/A Range: N/A Default value: N/A

Table 5-344 LoadBalancerRef

Parameter	Type	Description
id	String	Definition: Specifies the load balancer ID. Range: N/A

Table 5-345 Tag

Parameter	Type	Description
key	String	Definition: Specifies the tag key. Range: N/A
value	String	Definition: Specifies the tag value. Range: N/A

Table 5-346 ListenerIpGroup

Parameter	Type	Description
ipgroup_id	String	Definition: Specifies the ID of the IP address group associated with the listener. This parameter is mandatory during creation and is optional during update. Constraints: The specified IP address group must exist, and the value cannot be null . Otherwise, the IP address group conflicts with enable_ipgroup .
enable_ipgroup	Boolean	Definition: Specifies whether access control is enabled. A listener with access control enabled can be directly deleted. Range: • true: Access control is enabled. • false: Access control is disabled.

Parameter	Type	Description
type	String	Definition: Specifies how access to the listener is controlled. Range: • white: 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 5-347 ListenerQuicConfig

Parameter	Type	Description
quic_listener_id	String	Definition: Specifies the ID of the QUIC listener. Range: N/A
enable_quic_upgrade	Boolean	Definition: Specifies whether to enable QUIC upgrade. If this option is enabled, HTTPS listeners will be upgraded to QUIC listeners. Range: • True: Enable QUIC upgrade. • False: Disable QUIC upgrade.

Table 5-348 PortRange

Parameter	Type	Description
start_port	Integer	Definition: Specifies the start port number. Constraints: N/A Range: 1-65535 Default value: N/A
end_port	Integer	Definition: Specifies the end port number. The value must be greater than or equal to the start port number. Constraints: N/A Range: 1-65535 Default value: N/A

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.getenv("CLOUD_SDK_AK")
    sk = os.getenv("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 5-349 Path Parameters

Parameter	Mandatory	Type	Description
listener_id	Yes	String	Specifies the listener ID.
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-350 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-351 Request body parameters

Parameter	Mandatory	Type	Description
listener	Yes	UpdateListenerOption object	Definition: Specifies the request parameters for updating a listener. Constraints: N/A

Table 5-352 UpdateListenerOption

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Definition: Specifies the administrative status of the listener. Constraints: The value can only be updated to true . Range: N/A Default value: N/A
client_ca_tls_container_ref	No	String	Definition: Specifies the ID of the CA certificate used by the listener. Constraints: - This parameter is available only when type is set to client. - This parameter is not available if the listener protocol is QUIC. Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
default_pool_id	No	String	Definition: Specifies the ID of the default backend server group of the listener. If there is no matched forwarding policy, requests will be routed to the default backend server group. Constraints: N/A Range: N/A Default value: N/A
default_tls_container_ref	No	String	Definition: Specifies the ID of the server certificate used by the listener. Constraints: This parameter is mandatory when the listener protocol is HTTPS, and type must be set to server . Range: N/A Default value: N/A
description	No	String	Definition: Provides supplementary information about the listener. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
http2_enable	No	Boolean	Definition: Specifies whether to allow clients to use HTTP/2 to communicate with the load balancer for higher access performance. However, the load balancer still uses HTTP/1.x to forward requests to the backend server. Constraints: • This parameter is valid only for HTTPS listeners. • This parameter is not available for QUIC listeners and the response is fixed at true. • You can configure this parameter for listeners with other protocols, but it will not take effect. Range: N/A Default value: N/A
insert_headers	No	ListenerInsertHeaders object	Definition: Specifies the HTTP headers that can transmit required information to backend servers. For example, you can use the X-Forwarded-ELB-IP header to transmit the load balancer EIP to backend servers. Constraints: This parameter can be configured only for HTTP, HTTPS, and QUIC listeners.
name	No	String	Definition: Specifies the name of the listener. Constraints: If you leave the listener name empty, you cannot locate it in the listener list and view its details. Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
sni_container_refs	No	Array of strings	Definition: Specifies the IDs of SNI certificates (server certificates with domain names) used by the listener. Constraints: • QUIC listeners support only RSA certificates. • Each domain name of an SNI certificate must be unique. • The total number of domain names of all SNI certificates cannot exceed 200. Range: N/A Default value: N/A
sni_match_algo	No	String	Definition: Specifies how wildcard domain name matches with the SNI certificates used by the listener. Constraints: N/A Range: • longest_suffix: indicates longest suffix match. • wildcard: indicates wildcard match. Default value: wildcard

Parameter	Mandatory	Type	Description
tls_ciphers_policy	No	String	Definition: Specifies the security policy used by the listener. Constraints: • This parameter is available 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 takes 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). Range: tls-1-0-inherit, tls-1-0, tls-1-1, tls-1-2, 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. The default value is tls-1-2.

Parameter	Mandatory	Type	Description
security_policy_id	No	String	Definition: Specifies the ID of the custom security policy. Constraints: • This parameter is available only for HTTPS listeners added to a dedicated load balancer. • If both security_policy_id and tls_ciphers_policy are specified, only security_policy_id takes 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). Range: N/A Default value: N/A
enable_member_retry	No	Boolean	Definition: Specifies whether to enable health check retries for backend servers. Constraints: • 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. Range: true indicates health check retries will be enabled. false indicates health check retries will be disabled. Default value: N/A

Parameter	Mandatory	Type	Description
member_timeout	No	Integer	Definition: 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. Constraints: This parameter is available only for HTTP and HTTPS listeners. Range: 1-300s. Default value: 60s
client_timeout	No	Integer	Definition: Specifies the timeout duration for waiting for a request from a client, in seconds. This parameter is available only for HTTP and HTTPS listeners. Constraints: This parameter is unavailable for TCP and UDP listeners. Range: 1-300s Default value: 60s

Parameter	Mandatory	Type	Description
keepalive_timeout	No	Integer	Definition: Specifies the idle timeout duration, in seconds. If the load balancer receives no requests within the idle timeout duration, it will disconnect the connection with the client and establish a new connection when there is a new request. Constraints: This parameter is not supported by UDP listeners of shared load balancers. Range: • 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: 60s
ipgroup	No	UpdateListenerIpGroupOption object	Definition: Specifies the IP address group associated with the listener. Constraints: N/A

Parameter	Mandatory	Type	Description
transparent_client_ip_enable	No	Boolean	Definition: Specifies whether to pass source IP addresses of the clients to backend servers. If it is enabled, the source IP addresses of the clients will be passed to the backend server. This parameter applies only to TCP/UDP listeners added to a shared load balancer. Constraints: • If this function is enabled, the load balancer communicates with backend servers using client 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, the backend server specifications cannot be changed. Range: • 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. Default value: N/A

Parameter	Mandatory	Type	Description
proxy_protocol_enable	No	Boolean	Definition: Specifies whether to enable ProxyProtocol to pass the source IP addresses of the clients to backend servers. Constraints: This parameter is available only for TLS listeners and does not take effect for other types of listeners. Range: The value can be true (enable this option) or false (disable this option). Default value: false

Parameter	Mandatory	Type	Description
enhance_l7policy_enable	No	Boolean	Definition: Specifies whether to enable advanced forwarding. If advanced forwarding is enabled, more flexible forwarding policies and rules are supported. 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. Constraints: • Advanced forwarding cannot be disabled once it is enabled. • If advanced forwarding is enabled, forwarding policy priorities are defined by priority. The priorities are not automatically sorted. For details, see the description of the priority parameter in the forwarding policy.

Parameter	Mandatory	Type	Description
			Range: The value can be true (enable this option) or false (disable this option). Default value: false
quic_config	No	UpdateListenerQuicConfigOption object	Definition: Specifies the QUIC configuration for the current listener. Constraints: • 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. NOTE Suppose the client sends an HTTP request to the server and carries information indicating that the QUIC protocol is supported. If enable_quic_upgrade is set to true , the QUIC port and version information supported by the server will be included in the response header. When the client sends both HTTPS and QUIC requests, if the QUIC request is sent and responded, the client will use the QUIC protocol to communicate with the backend servers.
protection_status	No	String	Definition: Specifies the protection status. Constraints: N/A Range: • nonProtection (default): The resource is not protected. • consoleProtection: Modifications are not allowed on the console. Default value: N/A

Parameter	Mandatory	Type	Description
protection_reason	No	String	Definition: Specifies why modification protection is enabled. Constraints: This parameter is valid only when protection_status is set to consoleProtection . Range: The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>). Default value: N/A
gzip_enable	No	Boolean	Definition: Specifies whether to enable gzip_enable for a load balancer. Constraints: This parameter can be configured only for HTTP, HTTPS, and QUIC listeners. Range: N/A Default value: false
ssl_early_data_enable	No	Boolean	Definition: Specifies whether to enable zero round trip time resumption (0-RTT) for listeners. Constraints: 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 , there may be replay attacks. Range: N/A Default value: false

Parameter	Mandatory	Type	Description
cps	No	Integer	Definition: Specifies the maximum number of new connections that a listener can handle per second. Constraints: If the value is greater than the number defined in the load balancer flavors, the latter is used as the limit. Range: 0 to 1000000 Default value: 0, indicating that the number is not limited.
connection	No	Integer	Definition: Specifies the maximum number of concurrent connections that a listener can handle per second. Constraints: If the value is greater than the number defined in the load balancer flavors, the latter is used as the limit. Range: 0 to 1000000 Default value: 0, indicating that the number is not limited.
nat64_enable	No	Boolean	Definition: Specifies whether to translate between IPv4 and IPv6 addresses. This option allows 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 . Range: true: Enable nat64_enable . false: Disable nat64_enable . Default value: false

Table 5-353 ListenerInsertHeaders

Parameter	Mandatory	Type	Description
X-Forwarded-ELB-IP	No	Boolean	Definition: If X-Forwarded-ELB-IP is set to true , the load balancer EIP will be stored in the X-Forwarded-ELB-IP header and passed to backend servers. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-Port	No	Boolean	Definition: If X-Forwarded-Port is set to true , the listening port of the load balancer will be stored in the X-Forwarded-Port header and passed to backend servers. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-For-Port	No	Boolean	Definition: 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. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-Host	No	Boolean	Definition: If X-Forwarded-Host is set to true , the client host can be stored in the X-Forwarded-Host header and passed to backend servers. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
X-Forwarded-Proto	No	Boolean	Definition: If X-Forwarded-Proto is set to true , the listener protocol of the load balancer can be stored in the X-Forwarded-Proto header and passed to backend servers. Constraints: N/A Range: N/A Default value: N/A
X-Real-IP	No	Boolean	Definition: If X-Real-IP is set to true , the client IP address can be stored in the X-Real-IP header and passed to backend servers. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-ELB-ID	No	Boolean	Definition: If X-Forwarded-ELB-ID is set to true , the load balancer ID can be transferred to backend servers through the X-Forwarded-ELB-ID header. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-TLS-Certificate-ID	No	Boolean	Definition: 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 X-Forwarded-TLS-Certificate-ID header. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
X-Forwarded-TLS-Protocol	No	Boolean	Definition: If X-Forwarded-TLS-Protocol is set to true , the algorithm protocol of the load balancer can be transferred to backend servers through the X-Forwarded-TLS-Protocol header. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-TLS-Cipher	No	Boolean	Definition: If X-Forwarded-TLS-Cipher is set to true , the algorithm suite of the load balancer can be transferred to backend servers through the X-Forwarded-TLS-Cipher header. Constraints: N/A Range: N/A Default value: N/A

Table 5-354 UpdateListenerIpGroupOption

Parameter	Mandatory	Type	Description
ipgroup_id	No	String	Definition: Specifies the ID of the IP address group associated with the listener. This parameter is mandatory during creation and is optional during update. Constraints: The specified IP address group must exist, and the value cannot be null . Otherwise, the IP address group conflicts with enable_ipgroup . Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
enable_ipgroup	No	Boolean	Definition: Specifies whether to enable access control. A listener with access control enabled can be directly deleted. Constraints: N/A Range: • true: Enable access control. • false: Disable access control. Default value: N/A
type	No	String	Definition: Specifies how access to the listener is controlled. Constraints: N/A Range: • white: 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. Default value: N/A

Table 5-355 UpdateListenerQuicConfigOption

Parameter	Mandatory	Type	Description
quic_listener_id	No	String	Definition: Specifies the ID of the QUIC listener. Constraints: 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 . Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
enable_quic_upgrade	No	Boolean	Definition: Specifies whether to enable QUIC upgrade. If this option is enabled, HTTPS listeners will be upgraded to QUIC listeners. Constraints: N/A Range: • True: Enable QUIC upgrade. • False: Disable QUIC upgrade. Default value: N/A

Response Parameters

Status code: 200

Table 5-356 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
listener	Listener object	Definition: Specifies the listener information. Constraints: N/A

Table 5-357 Listener

Parameter	Type	Description
admin_state_up	Boolean	Definition: Specifies the administrative status of the listener. Default value: true
client_ca_tls_container_ref	String	Definition: Specifies the ID of the CA certificate used by the listener. This parameter is available only when type is set to client . Default value: N/A

Parameter	Type	Description
connection_limit	Integer	Definition: Specifies the maximum number of connections that the listener can establish with backend servers. Range: an integer greater than or equal to -1
created_at	String	Definition: Specifies the time when the listener was created. Range: N/A The value must be in the format of <i>yyyy-MM-dd"T"HH:mm:ss"Z"</i> , for example, 2021-07-30T12:03:44Z.
default_pool_id	String	Definition: Specifies the ID of the default backend server group of the listener. If there is no matched forwarding policy, requests will be routed to the default backend server group. Range: N/A
default_tls_container_ref	String	Definition: Specifies the ID of the server certificate used by the listener. Default value: N/A
description	String	Definition: Provides supplementary information about the listener. Range: N/A
http2_enable	Boolean	Definition: Specifies whether to allow clients to use HTTP/2 to communicate with the load balancer for higher access performance. However, the load balancer still uses HTTP/1.x to forward requests to the backend server. Range: N/A
id	String	Definition: Specifies the listener ID. Range: N/A
insert_headers	ListenerInsertHeaders object	Definition: Specifies the HTTP headers that can transmit required information to backend servers. For example, you can use the X-Forwarded-ELB-IP header to transmit the load balancer EIP to backend servers.

Parameter	Type	Description
loadbalancers	Array of LoadBalancerRef objects	Definition: Specifies the ID of the load balancer that the listener is added to. A listener can be associated with only one load balancer.
name	String	Definition: Specifies the name of the listener. If you leave the listener name empty, you cannot locate it in the listener list and view its details. Range: N/A
project_id	String	Definition: Specifies the ID of the project that the listener belongs to. Range: N/A
enterprise_project_id	String	Definition: Specifies the enterprise project ID. Range: N/A
protocol	String	Definition: Specifies the protocol of the listener. Range: TCP, UDP, HTTP, HTTPS, TERMINATED_HTTPS, QUIC, or TLS.
protocol_port	Integer	Definition: Specifies the port used by the listener. Default value: N/A
sni_container_refs	Array of strings	Definition: Specifies the IDs of SNI certificates (server certificates with domain names) used by the listener. Range: N/A
sni_match_algo	String	Definition: Specifies how wildcard domain name matches with the SNI certificates used by the listener. Range: longest_suffix indicates longest suffix match. wildcard indicates wildcard match.
tags	Array of Tag objects	Definition: Lists the tags.
updated_at	String	Definition: Specifies the time when the listener was updated. Range: The value must be in the format of <i>yyyy-MM-dd"T"HH:mm:ss"Z"</i> , for example, 2021-07-30T12:03:44Z.

Parameter	Type	Description
tls_ciphers_policy	String	Definition: Specifies the security policy used by the listener. Range: tls-1-0-inherit, tls-1-0, tls-1-1, tls-1-2, 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. The default value is tls-1-2.
security_policy_id	String	Definition: Specifies the ID of the custom security policy. Range: N/A
enable_member_retry	Boolean	Definition: Specifies whether to enable health check retries for backend servers. Range: true indicates health check retries will be enabled. false indicates health check retries will be disabled.
keepalive_timeout	Integer	Definition: Specifies the idle timeout duration, in seconds. If the load balancer receives no requests within the idle timeout duration, it will disconnect the connection with the client and establish a new connection when there is a new request. Range: - For TCP listeners, the value ranges from 10s to 4000s. - For HTTP, HTTPS, and TERMINATED_HTTPS listeners, the value ranges from 0s to 4000s.
client_timeout	Integer	Definition: 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. Range: 1-300

Parameter	Type	Description
member_timeout	Integer	Definition: 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. Range: 1-300
ipgroup	ListenerIpGroup object	Definition: Specifies the IP address group associated with the listener.
transparent_client_ip_enable	Boolean	Definition: Specifies whether to pass source IP addresses of the clients to backend servers. If it is enabled, the source IP addresses of the clients will be passed to the backend server. This parameter applies only to TCP/UDP listeners added to a shared load balancer. Range: • 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.
proxy_protocol_enable	Boolean	Definition: Specifies whether to enable ProxyProtocol 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. Range: The value can be true (enable this option) or false (disable this option).

Parameter	Type	Description
enhance_l7policy_enable	Boolean	Definition: Specifies whether to enable advanced forwarding. If advanced forwarding is enabled, more flexible forwarding policies and rules are supported. 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. Range: The value can be true (enable this option) or false (disable this option).
quic_config	ListenerQuicConfig object	Definition: Specifies the QUIC configuration for the current listener.
protection_status	String	Definition: Specifies the protection status. Range: • nonProtection: The resource is not protected. • consoleProtection: Modification is not allowed on the console.
protection_reason	String	Definition: Specifies why modification protection is enabled. Range: The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).

Parameter	Type	Description
gzip_enable	Boolean	Definition: Specifies whether to enable gzip_enable for a load balancer. Range: The value can be true (enable this option) or false (disable this option).
port_ranges	Array of PortRange objects	Definition: Specifies one or more port ranges, including the start and end ports.
ssl_early_data_enable	Boolean	Definition: Specifies whether to enable zero round trip time resumption (0-RTT) for listeners. Constraints: This option can be configured only for HTTPS listeners and depends on the TLS 1.3 security policy protocols.
cps	Integer	Definition: Specifies the maximum number of new connections that a listener can handle per second. If the value is greater than the number defined in the load balancer flavors, the latter is used as the limit. Range: 0 to 1000000
connection	Integer	Definition: Specifies the maximum number of concurrent connections that a listener can handle per second. If the value is greater than the number defined in the load balancer flavors, the latter is used as the limit. Range: 0 to 1000000
nat64_enable	Boolean	Definition: Specifies whether to translate between IPv4 and IPv6 addresses. This option allows a client to access IPv4 or IPv6 backend servers by accessing the IPv4 or IPv6 address of a load balancer. Range: true: Enable nat64_enable . false: Disable nat64_enable .

Table 5-358 ListenerInsertHeaders

Parameter	Type	Description
X-Forwarded-ELB-IP	Boolean	Definition: If X-Forwarded-ELB-IP is set to true , the load balancer EIP will be stored in the X-Forwarded-ELB-IP header and passed to backend servers. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-Port	Boolean	Definition: If X-Forwarded-Port is set to true , the listening port of the load balancer will be stored in the X-Forwarded-Port header and passed to backend servers. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-For-Port	Boolean	Definition: 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. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-Host	Boolean	Definition: If X-Forwarded-Host is set to true , the client host can be stored in the X-Forwarded-Host header and passed to backend servers. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-Proto	Boolean	Definition: If X-Forwarded-Proto is set to true , the listener protocol of the load balancer can be stored in the X-Forwarded-Proto header and passed to backend servers. Constraints: N/A Range: N/A Default value: N/A

Parameter	Type	Description
X-Real-IP	Boolean	Definition: If X-Real-IP is set to true , the client IP address can be stored in the X-Real-IP header and passed to backend servers. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-ELB-ID	Boolean	Definition: If X-Forwarded-ELB-ID is set to true , the load balancer ID can be transferred to backend servers through the X-Forwarded-ELB-ID header. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-TLS-Certificate-ID	Boolean	Definition: 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 X-Forwarded-TLS-Certificate-ID header. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-TLS-Protocol	Boolean	Definition: If X-Forwarded-TLS-Protocol is set to true , the algorithm protocol of the load balancer can be transferred to backend servers through the X-Forwarded-TLS-Protocol header. Constraints: N/A Range: N/A Default value: N/A
X-Forwarded-TLS-Cipher	Boolean	Definition: If X-Forwarded-TLS-Cipher is set to true , the algorithm suite of the load balancer can be transferred to backend servers through the X-Forwarded-TLS-Cipher header. Constraints: N/A Range: N/A Default value: N/A

Table 5-359 LoadBalancerRef

Parameter	Type	Description
id	String	Definition: Specifies the load balancer ID. Range: N/A

Table 5-360 Tag

Parameter	Type	Description
key	String	Definition: Specifies the tag key. Range: N/A
value	String	Definition: Specifies the tag value. Range: N/A

Table 5-361 ListenerIpGroup

Parameter	Type	Description
ipgroup_id	String	Definition: Specifies the ID of the IP address group associated with the listener. This parameter is mandatory during creation and is optional during update. Constraints: The specified IP address group must exist, and the value cannot be null . Otherwise, the IP address group conflicts with enable_ipgroup .
enable_ipgroup	Boolean	Definition: Specifies whether access control is enabled. A listener with access control enabled can be directly deleted. Range: • true: Access control is enabled. • false: Access control is disabled.

Parameter	Type	Description
type	String	Definition: Specifies how access to the listener is controlled. Range: • white: 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 5-362 ListenerQuicConfig

Parameter	Type	Description
quic_listener_id	String	Definition: Specifies the ID of the QUIC listener. Range: N/A
enable_quic_upgrade	Boolean	Definition: Specifies whether to enable QUIC upgrade. If this option is enabled, HTTPS listeners will be upgraded to QUIC listeners. Range: • True: Enable QUIC upgrade. • False: Disable QUIC upgrade.

Table 5-363 PortRange

Parameter	Type	Description
start_port	Integer	Definition: Specifies the start port number. Constraints: N/A Range: 1-65535 Default value: N/A
end_port	Integer	Definition: Specifies the end port number. The value must be greater than or equal to the start port number. Constraints: N/A Range: 1-65535 Default value: N/A

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.ElClientBuilder().
            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 5-364 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
listener_id	Yes	String	Specifies the listener ID.

Request Parameters

Table 5-365 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 204

Successful request.

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.ElClientBuilder().
            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 5-366 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
listener_id	Yes	String	Specifies the listener ID.

Request Parameters

Table 5-367 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 204

Successful request.

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	Successful request.

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 5-368 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-369 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-370 Request body parameters

Parameter	Mandatory	Type	Description
pool	Yes	CreatePoolOption object	Definition: Specifies the request parameters for creating a backend server group. Constraints: N/A

Table 5-371 CreatePoolOption

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Definition: Specifies the administrative status of the backend server group. Constraints: The value can only be true . Range: true Default value: true
az_affinity	No	AzAffinity object	Definition: Specifies how AZ affinity is configured for the backend server group. Constraints: N/A
description	No	String	Definition: Provides supplementary information about the backend server group. Constraints: N/A Range: N/A Default value: N/A
lb_algorithm	Yes	String	Definition: Specifies the load balancing algorithm used by the load balancer to route requests to backend servers in the associated backend server group. Constraints: • If the value is SOURCE_IP or QUIC_CID, the weights of backend servers in the backend server group are invalid. • QUIC_CID is available only when the protocol of the backend server group is QUIC. Range: • ROUND_ROBIN: weighted round robin • LEAST_CONNECTIONS: weighted least connections • SOURCE_IP: source IP hash • QUIC_CID: connection ID Default value: N/A

Parameter	Mandatory	Type	Description
listener_id	No	String	Definition: Specifies the ID of the listener with which the backend server group is associated. Constraints: - At least one of listener_id, loadbalancer_id, and type must be specified. - You do not need to specify listener_id and loadbalancer_id for the backend server group of a dedicated load balancer, but must specify at least one for a shared load balancer. Range: N/A Default value: N/A
loadbalancer_id	No	String	Definition: Specifies the ID of the load balancer with which the backend server group is associated. Constraints: - At least one of listener_id, loadbalancer_id, and type must be specified. - You do not need to specify listener_id and loadbalancer_id for the backend server group of a dedicated load balancer, but must specify at least one for a shared load balancer. Range: N/A Default value: N/A
name	No	String	Definition: Specifies the backend server group name. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
project_id	No	String	Definition: Specifies the project ID of the backend server group. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
protocol	Yes	String	Definition: Specifies the protocol used by the backend server group to receive requests. Constraints: • 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 must 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 must 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, ip_version must be set to v4. • If the backend server group's protocol is QUIC, session_persistence must be set to true and type set to SOURCE_IP. • If the backend server group's protocol is GRPC, http2_enable of the listener must be set to true.

Parameter	Mandatory	Type	Description
			Range: TCP, UDP, TLS, HTTP, HTTPS, GRPC, or QUIC Default value: N/A
session_persistence	No	CreatePoolSessionPersistenceOption object	Definition: Specifies the sticky session. Constraints: Slow start and sticky session cannot be enabled at the same time. If both are enabled, sticky session will be invalid.
slow_start	No	CreatePoolSlowStartOption object	Definition: 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. Constraints: • This parameter is valid only when the backend server group protocol is HTTP, HTTPS, or GRPC. For other protocols, an error will be reported. • Slow start and sticky session cannot be enabled at the same time. If both are enabled, sticky session will be invalid.

Parameter	Mandatory	Type	Description
member_deletion_protection_enable	No	Boolean	Definition: Whether to enable removal protection for the backend server. Once the option is enabled, backend servers cannot be removed from the backend server group. Constraints: Once the option is enabled, an error will be returned when the following APIs are called to: • Delete a load balancer and its associated resources (DELETE /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}/force-elb). • Delete a load balancer and its associated EIPs (POST /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}/delete-cascade). • Delete a listener and its associated resources (DELETE /v3/{project_id}/elb/listeners/{listener_id}/force). • Delete a backend server group and its associated resources (DELETE /v3/{project_id}/elb/pools/{pool_id}/delete-cascade). • Remove a backend server (DELETE /v3/{project_id}/elb/pools/{pool_id}/members/{member_id}). • Remove backend servers in batches (POST /v3/{project_id}/elb/pools/{pool_id}/members/batch-delete). Range: false (disable this option) or true (enable this option).

Parameter	Mandatory	Type	Description
			Default value: false NOTE Disable deletion protection or removal protection for your resources before deregistering your account.
vpc_id	No	String	Definition: Specifies the ID of the VPC where the backend server group works. Constraints: • 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. Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
type	No	String	Definition: Specifies the backend server group type. Constraints: • If this parameter is not passed, any type of backend servers can be added. type will be returned as an empty string. • At least one of listener_id, loadbalancer_id, and type must be specified. • You do not need to specify listener_id and loadbalancer_id for the backend server group of a dedicated load balancer, but must specify at least one for a shared load balancer. Range: • 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. Default value: N/A
ip_version	No	String	Definition: Specifies the IP address version supported by the backend server group. Constraints: N/A 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. Default value: N/A

Parameter	Mandatory	Type	Description
protection_status	No	String	Definition: Specifies the protection status. Constraints: N/A Range: • nonProtection: The resource is not protected. • consoleProtection: Modification is not allowed on the console. Default value: nonProtection
protection_reason	No	String	Definition: Specifies why modification protection is enabled. Constraints: This parameter is valid only when protection_status is set to consoleProtection . Range: The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>). Default value: N/A
any_port_enable	No	Boolean	Definition: 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 . Constraints: This option is available only for TCP, UDP, or QUIC backend server groups. Range: false (disable this option) or true (enable this option). Default value: N/A

Parameter	Mandatory	Type	Description
connection_drain	No	ConnectionDrain object	Definition: Specifies the configurations of deregistration delay. 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. Constraints: This parameter is only available for TCP, UDP, and QUIC backend server groups and TCP and UDP listeners.
pool_health	No	PoolHealth object	Specifies the configurations of the pool health feature. Constraints: N/A
public_border_group	No	String	Definition: Specifies the public border group. Constraints: N/A Range: • center: public border group of the central site • Edge site name: public border group of an edge site Default value: N/A
quic_cid_hash_strategy	No	QuicCidHashStrategy object	Definition: Specifies multi-path forwarding configuration based on destination connection IDs. Constraints: N/A

Table 5-372 AzAffinity

Parameter	Mandatory	Type	Description
enable	Yes	Boolean	Definition: Specifies whether to enable AZ affinity for the backend server group. If this parameter is set to true, ELB forwards traffic across the backend servers in the same AZ as the load balancer. Constraints: • This parameter is available only for IP, TCP, and UDP backend server groups. • This parameter is not available for backend server groups that are associated with TLS listeners. • If the parameter is set to true, parameter pool_health will be ignored. Range: false (disable this option) or true (enable this option). Default value: N/A

Parameter	Mandatory	Type	Description
az_minimum_healthy_member_percentage	No	Integer	Definition: Specifies a percentage that is used to determine the health of an AZ. If the percentage of healthy servers in the AZ of the load balancer falls below the specified value, az_unhealthy_fallback_strategy is triggered. az_minimum_healthy_member_percentage shows the percentage of backend servers that are healthy in a backend server group of an AZ. The number of healthy servers is rounded up. For example, in AZ A, if there are three backend servers in the backend server group and az_minimum_healthy_member_percentage is set to 66%, the number of healthy servers is rounded up to 2 ($3 \times 0.66 = 1.98$). If there are fewer than two healthy servers in AZ A, az_unhealthy_fallback_strategy is triggered. If az_minimum_healthy_member_percentage is set to 67%, the number of healthy servers is rounded up to 3 ($3 \times 0.67 = 2.01$). If there are fewer than three healthy servers in AZ A, az_unhealthy_fallback_strategy is triggered. Constraints: • If enable is set to true, az_minimum_healthy_member_percentage and az_minimum_healthy_member_count cannot be set to -1 at the same time. • If enable is set to true, either az_minimum_healthy_member_percentage or az_minimum_healthy_member_count must be set to -1.

Parameter	Mandatory	Type	Description
			Range: an integer ranging from -1 to 100. An integer from 0 to 100 indicates the percentage of healthy servers in the AZ of the load balancer. -1 indicates that az_minimum_healthy_member_count takes effect. Default value: N/A
az_minimum_healthy_member_count	No	Integer	Definition: Specifies a number that is used to determine the health of an AZ. If the number of healthy servers in the AZ of the load balancer falls below the specified value, az_unhealthy_fallback_strategy is triggered. az_minimum_healthy_member_count shows the number of healthy servers in a backend server group of an AZ. Constraints: • If enable is set to true, az_minimum_healthy_member_percentage and az_minimum_healthy_member_count cannot be set to -1 at the same time. • If enable is set to true, either az_minimum_healthy_member_percentage or az_minimum_healthy_member_count must be set to -1. Range: an integer ranging from -1 to 10000. An integer from 0 to 10000 indicates the number of healthy servers in the AZ of the load balancer. -1 indicates that az_minimum_healthy_member_percentage takes effect. Default value: N/A

Parameter	Mandatory	Type	Description
az_unhealthy_fallback_strategy	No	String	Definition: Specifies how traffic will be distributed across backend servers in an AZ if the percentage or number of healthy servers in the AZ of the load balancer falls below the specified value. Range: • forward_to_all_member_of_local_az: forwards requests across all backend servers in the same AZ as the load balancer, even if some servers are unhealthy. • forward_to_healthy_member_of_remote_az: forwards requests across healthy backend servers in different AZs from the load balancer. • forward_to_all_healthy_member: forwards requests across healthy backend servers in all AZs. • forward_to_all_member: forwards requests across all backend servers in all AZs, even if some servers are unhealthy. Constraints: N/A Default value: forward_to_all_member_of_local_az

Table 5-373 CreatePoolSessionPersistenceOption

Parameter	Mandatory	Type	Description
cookie_name	No	String	Definition: Specifies the cookie name. Constraints: This parameter takes effect only when type is set to APP_COOKIE. Otherwise, an error will be returned. Range: The value can contain a maximum of 1,024 characters. Default value: N/A
type	Yes	String	Definition: Specifies the sticky session type. Constraints: - 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, only HTTP_COOKIE and APP_COOKIE take effect. - If the backend server group's protocol is QUIC, session_persistence must be set to true and type set to SOURCE_IP. Range: SOURCE_IP , HTTP_COOKIE , or APP_COOKIE . Default value: N/A

Parameter	Mandatory	Type	Description
persistence_timeout	No	Integer	Definition: Specifies the stickiness duration, in minutes. Constraints: This parameter will not take effect when type is set to APP_COOKIE . Range: - 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. Default value: N/A

Table 5-374 CreatePoolSlowStartOption

Parameter	Mandatory	Type	Description
enable	No	Boolean	Definition: Specifies whether to enable slow start. Constraints: N/A Range: true: This option will be enabled. false: This option will be disabled. Default value: false
duration	No	Integer	Definition: Specifies the slow start duration, in seconds. Constraints: N/A Range: 30 to 1200, in seconds. Default value: 30

Table 5-375 ConnectionDrain

Parameter	Mandatory	Type	Description
enable	No	Boolean	Definition: Specifies whether to enable connection_drain . Constraints: N/A Range: The value can be true (enable this option) or false (disable this option). Default value: N/A
timeout	No	Integer	Definition: Specifies the deregistration delay timeout, in seconds. Constraints: N/A Range: 10 to 4000, in seconds. Constraints: N/A

Table 5-376 PoolHealth

Parameter	Mandatory	Type	Description
minimum_healthy_member_count	No	Integer	Definition: Specifies the number of healthy backend servers below which the backend server group is considered as unhealthy. Range: • 0 (default): pool_health does not take effect. • 1: pool_health takes effect.

Table 5-377 QuicCidHashStrategy

Parameter	Mandatory	Type	Description
len	Yes	Integer	Definition: Specifies the length of the hash factor in the connection ID. Constraints: This parameter is valid only when the load balancing algorithm is QUIC_CID . Range: 1 to 20 Default value: 3

Parameter	Mandatory	Type	Description
offset	Yes	Integer	Definition: Specifies the start position in the connection ID as the hash factor. Constraints: This parameter is valid only when the load balancing algorithm is QUIC_CID . Range: 0 to 19 Default value: 1

Response Parameters

Status code: 201

Table 5-378 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
pool	Pool object	Definition: Specifies the backend server group.

Table 5-379 Pool

Parameter	Type	Description
admin_state_up	Boolean	Definition: Specifies the administrative status of the backend server group. The value can only be true . Range: true (enabled)
az_affinity	AzAffinity object	Definition: Specifies how AZ affinity is configured for the backend server group.
description	String	Definition: Provides supplementary information about the backend server group. Range: N/A

Parameter	Type	Description
healthmonitor_id	String	Definition: Specifies the ID of the health check configured for the backend server group. Range: N/A
id	String	Definition: Specifies the backend server group ID. Range: N/A
lb_algorithm	String	Definition: Specifies the load balancing algorithm used by the load balancer to route requests to backend servers in the associated backend server group. Range: • ROUND_ROBIN: weighted round robin • LEAST_CONNECTIONS: weighted least connections • SOURCE_IP: source IP hash • QUIC_CID: connection ID
listeners	Array of ListenerRef objects	Definition: Specifies the IDs of the listeners with which the backend server group is associated.
loadbalancers	Array of LoadBalancerRef objects	Definition: Specifies the IDs of the load balancers with which the backend server group is associated.
members	Array of MemberRef objects	Definition: Specifies the IDs of backend servers in the backend server group.
name	String	Definition: Specifies the backend server group name. Range: N/A
project_id	String	Definition: Specifies the project ID of the backend server group. Range: N/A
protocol	String	Definition: Specifies the protocol used by the backend server group to receive requests from the load balancer. Constraints: N/A Range: The value can be TCP , UDP , TLS , HTTP , HTTPS , GRPC , or QUIC . Default value: N/A

Parameter	Type	Description
session_persistence	SessionPersistence object	Definition: Specifies the sticky session.
ip_version	String	Definition: Specifies the IP address version supported by the backend server group. 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	Definition: 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.
member_deletion_protection_enable	Boolean	Definition: Whether to enable removal protection for the backend server. Once the option is enabled, backend servers cannot be removed from the backend server group. Range: false (disable this option) or true (enable this option). NOTE Disable deletion protection or removal protection for your resources before deregistering your account.
created_at	String	Definition: Specifies the creation time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format. Note: This parameter 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	Definition: Specifies the update time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format. Note: This parameter 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	Definition: Specifies the ID of the VPC where the backend server group works. Range: N/A
type	String	Definition: Specifies the backend server group type. Range: • 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	Definition: Specifies the protection status. Range: • nonProtection: The resource is not protected. • consoleProtection: Modification is not allowed on the console.
protection_reason	String	Definition: Specifies why modification protection is enabled. Range: The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).

Parameter	Type	Description
any_port_enable	Boolean	Definition: 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 . Constraints: This option is available only for TCP, UDP, or QUIC backend server groups.
connection_drain	ConnectionDrain object	Definition: Specifies the configurations of deregistration delay. 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	Definition: Specifies the ID of the enterprise project. Range: • 0: The resource belongs to the default enterprise project. • A string in UUID format indicates a non-default enterprise project.
pool_health	PoolHealth object	Definition: Specifies the configurations of the pool health feature.
public_border_group	String	Definition: Specifies the public border group. Range: • center: public border group of the central site • Edge site name: public border group of an edge site
quic_cid_hash_strategy	QuicCidHashStrategy object	Definition: Specifies multi-path distribution configuration based on destination connection IDs.

Table 5-380 AzAffinity

Parameter	Type	Description
enable	Boolean	Definition: Specifies whether to enable AZ affinity for the backend server group. If this parameter is set to true, ELB forwards traffic across the backend servers in the same AZ as the load balancer. Constraints: • This parameter is available only for IP, TCP, and UDP backend server groups. • This parameter is not available for backend server groups that are associated with TLS listeners. • If the parameter is set to true, parameter pool_health will be ignored. Range: false (disable this option) or true (enable this option). Default value: N/A

Parameter	Type	Description
az_minimum_healthy_member_percentage	Integer	Definition: Specifies a percentage that is used to determine the health of an AZ. If the percentage of healthy servers in the AZ of the load balancer falls below the specified value, az_unhealthy_fallback_strategy is triggered. az_minimum_healthy_member_percentage shows the percentage of backend servers that are healthy in a backend server group of an AZ. The number of healthy servers is rounded up. For example, in AZ A, if there are three backend servers in the backend server group and az_minimum_healthy_member_percentage is set to 66%, the number of healthy servers is rounded up to 2 ($3 \times 0.66 = 1.98$). If there are fewer than two healthy servers in AZ A, az_unhealthy_fallback_strategy is triggered. If az_minimum_healthy_member_percentage is set to 67%, the number of healthy servers is rounded up to 3 ($3 \times 0.67 = 2.01$). If there are fewer than three healthy servers in AZ A, az_unhealthy_fallback_strategy is triggered. Constraints: • If enable is set to true, az_minimum_healthy_member_percentage and az_minimum_healthy_member_count cannot be set to -1 at the same time. • If enable is set to true, either az_minimum_healthy_member_percentage or az_minimum_healthy_member_count must be set to -1. Range: an integer ranging from -1 to 100. An integer from 0 to 100 indicates the percentage of healthy servers in the AZ of the load balancer. -1 indicates that az_minimum_healthy_member_count takes effect. Default value: N/A

Parameter	Type	Description
az_minimum_healthy_member_count	Integer	Definition: Specifies a number that is used to determine the health of an AZ. If the number of healthy servers in the AZ of the load balancer falls below the specified value, az_unhealthy_fallback_strategy is triggered. az_minimum_healthy_member_count shows the number of healthy servers in a backend server group of an AZ. Constraints: • If enable is set to true, az_minimum_healthy_member_percentage and az_minimum_healthy_member_count cannot be set to -1 at the same time. • If enable is set to true, either az_minimum_healthy_member_percentage or az_minimum_healthy_member_count must be set to -1. Range: an integer ranging from -1 to 10000. An integer from 0 to 10000 indicates the number of healthy servers in the AZ of the load balancer. -1 indicates that az_minimum_healthy_member_percentage takes effect. Default value: N/A

Parameter	Type	Description
az_unhealthy_fall_back_strategy	String	Definition: Specifies how traffic will be distributed across backend servers in an AZ if the percentage or number of healthy servers in the AZ of the load balancer falls below the specified value. Range: • forward_to_all_member_of_local_az: forwards requests across all backend servers in the same AZ as the load balancer, even if some servers are unhealthy. • forward_to_healthy_member_of_remote_az: forwards requests across healthy backend servers in different AZs from the load balancer. • forward_to_all_healthy_member: forwards requests across healthy backend servers in all AZs. • forward_to_all_member: forwards requests across all backend servers in all AZs, even if some servers are unhealthy. Constraints: N/A Default value: forward_to_all_member_of_local_az

Table 5-381 ListenerRef

Parameter	Type	Description
id	String	Definition: Specifies the listener ID. Range: N/A

Table 5-382 LoadBalancerRef

Parameter	Type	Description
id	String	Definition: Specifies the load balancer ID. Range: N/A

Table 5-383 MemberRef

Parameter	Type	Description
id	String	Specifies the backend server ID. Range: N/A

Table 5-384 SessionPersistence

Parameter	Type	Description
cookie_name	String	Definition: Specifies the cookie name. Range: The value can contain a maximum of 1,024 characters.
type	String	Definition: Specifies the sticky session type. Range: SOURCE_IP , HTTP_COOKIE , or APP_COOKIE .
persistence_timeout	Integer	Definition: Specifies the stickiness duration, in minutes. This parameter will not take effect when type is set to APP_COOKIE . Range: - 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 5-385 SlowStart

Parameter	Type	Description
enable	Boolean	Definition: Specifies whether to enable slow start. Range: true: This option will be enabled. false: This option will be disabled.
duration	Integer	Definition: Specifies the slow start duration, in seconds. Range: 30 to 1200, in seconds.

Table 5-386 ConnectionDrain

Parameter	Type	Description
enable	Boolean	Definition: Specifies whether to enable connection_drain . Constraints: N/A Range: The value can be true (enable this option) or false (disable this option). Default value: N/A
timeout	Integer	Definition: Specifies the deregistration delay timeout, in seconds. Constraints: N/A Range: 10 to 4000, in seconds. Constraints: N/A

Table 5-387 PoolHealth

Parameter	Type	Description
minimum_healthy_member_count	Integer	Definition: Specifies the number of healthy backend servers below which the backend server group is considered as unhealthy. Range: • 0 (default): pool_health does not take effect. • 1: pool_health takes effect.

Table 5-388 QuicCidHashStrategy

Parameter	Type	Description
len	Integer	Definition: Specifies the length of the hash factor in the connection ID. Constraints: This parameter is valid only when the load balancing algorithm is QUIC_CID . Range: 1 to 20 Default value: 3

Parameter	Type	Description
offset	Integer	Definition: Specifies the start position in the connection ID as the hash factor. Constraints: This parameter is valid only when the load balancing algorithm is QUIC_CID . 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

Successful request.

```
{
  "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.ElClientBuilder().
        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.ElClientBuilder().
            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	Successful request.

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 5-389 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Table 5-390 Query Parameters

Parameter	Mandatory	Type	Description
marker	No	String	Definition: Specifies the ID of the last record on the previous page. Constraints: • This parameter must be used together with limit. • If the parameter is not specified, only resources on the first page are queried. • This parameter cannot be left blank or set to an invalid ID. Range: N/A Default value: N/A
limit	No	Integer	Definition: Specifies the number of records returned on each page. Constraints: N/A Range: 0 to 2000 Default value: 2000

Parameter	Mandatory	Type	Description
page_reverse	No	Boolean	Definition: Specifies whether to use reverse query. Constraints: • This parameter must be used together with limit. • If page_reverse is set to true and you want to query the resources on the previous page, set the value of marker to the value of previous_marker. Range: • true: Query resources on the previous page. • false: Query resources on the next page. Default value: false
description	No	Array of strings	Definition: Specifies supplementary information about the backend server group. Multiple descriptions can be used for query in the format of <i>description=xxx&description=xx</i> . Constraints: N/A Range: N/A Default value: N/A
admin_state_up	No	Boolean	Definition: Specifies the administrative status of the backend server group. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
healthmonitor_id	No	Array of strings	Definition: Specifies the ID of the health check configured for the backend server group. Multiple IDs can be used for query in the format of <i>healthmonitor_id=xxx&healthmonitor_id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
id	No	Array of strings	Definition: Specifies the ID of the backend server group. Multiple IDs can be used for query in the format of <i>id=xxx&id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
name	No	Array of strings	Definition: Specifies the backend server group name. Multiple names can be used for query in the format of <i>name=xxx&name=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
loadbalancer_id	No	Array of strings	Definition: Specifies the ID of the load balancer with which the backend server group is associated. Multiple IDs can be used for query in the format of <i>loadbalancer_id=xxx&loadbalancer_id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
protocol	No	Array of strings	Definition: Specifies the protocol used by the backend server group to receive requests from the load balancer. Multiple protocols can be used for query in the format of <i>protocol=xxx&protocol=xxx</i> . Constraints: N/A Range: The value can be TCP , UDP , TLS , HTTP , HTTPS , GRPC , or QUIC . Default value: N/A
lb_algorithm	No	Array of strings	Definition: Specifies the load balancing algorithm used by the load balancer to route requests to backend servers in the associated backend server group. Multiple algorithms can be used for query in the format of <i>lb_algorithm=xxx&lb_algorithm=xxx</i> . Constraints: N/A Range: ● ROUND_ROBIN: weighted round robin ● LEAST_CONNECTIONS: weighted least connections ● SOURCE_IP: source IP hash ● QUIC_CID: connection ID Default value: N/A

Parameter	Mandatory	Type	Description
enterprise_project_id	No	Array of strings	Definition: Specifies the ID of the enterprise project. Multiple values can be used for query in the format of: <i>enterprise_project_id=xxx&enterprise_project_id=xxx</i>. Constraints: • If enterprise_project_id is not specified, resources in all enterprise projects are queried by default. Fine-grained authorization is performed. The elb:poools: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:poools:list permission are queried. Range: N/A Default value: N/A
ip_version	No	Array of strings	Definition: Specifies the IP address version supported by the backend server group. Multiple versions can be used for query in the format of <i>ip_version=xxx&ip_version=xxx</i>. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
member_address	No	Array of strings	Definition: Specifies the IP address of the backend server. This is a query parameter and will not be included in the response. Multiple IP addresses can be used for query in the format of <i>member_address=xxx&member_address=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
member_device_id	No	Array of strings	Definition: Specifies the ID of the ECS 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 used for query in the format of <i>member_device_id=xxx&member_device_id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
member_deletion_protection_enable	No	Boolean	Definition: Specifies whether to enable deletion protection. Constraints: N/A Range: false (disable this option) or true (enable this option). All resources will be queried if this parameter is not passed. Default value: N/A

Parameter	Mandatory	Type	Description
listener_id	No	Array of strings	Definition: Specifies the IDs of the associated listeners, including the listeners associated through forwarding policies. Multiple IDs can be used for query in the format of <i>listener_id=xxx&listener_id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
member_instance_id	No	Array of strings	Definition: Specifies the backend server ID. This is a query parameter and will not be included in the response. Multiple IDs can be used for query in the format of <i>member_instance_id=xxx&member_instance_id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
vpc_id	No	Array of strings	Definition: Specifies the ID of the VPC where the backend server group works. Constraints: N/A Range: N/A Default value: N/A
type	No	Array of strings	Definition: Specifies the type of the backend server group. Constraints: N/A Range: • 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. Default value: N/A

Parameter	Mandatory	Type	Description
protection_status	No	Array of strings	Definition: Specifies the protection status. Constraints: N/A Range: • nonProtection: The resource is not protected. • consoleProtection: Modification is not allowed on the console. Default value: N/A
connection_drain	No	Boolean	Definition: Specifies a connection_drain value for query, in the format of connection_drain=true or connection_drain=false . Constraints: N/A Range: N/A Default value: N/A
pool_health	No	String	Definition: Specifies a pool_health value for query, in the format of minimum_healthy_member_count=0 or minimum_healthy_member_count=1 . Constraints: N/A Range: N/A Default value: N/A
any_port_enable	No	Boolean	Definition: Specifies whether any_port_enable is enabled. If this option is enabled, the listener routes the requests to the backend server over the same port as the frontend port. Constraints: N/A Range: The value can be true (enabled) or false (disabled). Default value: N/A

Parameter	Mandatory	Type	Description
public_border_group	No	String	Definition: Specifies the public border group. Multiple public border groups can be queried in the format of <i>public_border_group=xxx&public_border_group=xxx</i> . Constraints: N/A Range: • center: public border group of the central site • Edge site name: public border group of an edge site Default value: N/A
quic_cid_len	No	Integer	Definition: 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 used for query in the format of <i>quic_cid_len=3&quic_cid_len=5</i> . Constraints: N/A Range: N/A Default value: N/A
quic_cid_offset	No	Integer	Definition: 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 used for query in the format of <i>quic_cid_offset=1&quic_cid_offset=3</i> . Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
az_affinity	No	Array of strings	Definition: Specifies whether AZ affinity of a backend server group is enabled. The following is an example: "az_affinity": { "enable": "true" } Multiple values can be used for query in the format of <i>az_affinity=enable=true&az_affinity=enable=false</i> . Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-391 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-392 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
page_info	PageInfo object	Definition: Specifies the pagination information.

Parameter	Type	Description
pools	Array of Pool objects	Definition: Lists the backend server groups.

Table 5-393 PageInfo

Parameter	Type	Description
previous_marker	String	Definition: Specifies the ID of the first record in the pagination query result. If page_reverse is set to true , this parameter is used together to query resources on the previous page. Range: N/A
next_marker	String	Definition: Specifies the ID of the last record in the pagination query result. It is usually used to query resources on the next page. Range: N/A
current_count	Integer	Definition: Specifies the number of records returned on the current page. Range: N/A

Table 5-394 Pool

Parameter	Type	Description
admin_state_up	Boolean	Definition: Specifies the administrative status of the backend server group. The value can only be true . Range: true (enabled)
az_affinity	AzAffinity object	Definition: Specifies how AZ affinity is configured for the backend server group.
description	String	Definition: Provides supplementary information about the backend server group. Range: N/A
healthmonitor_id	String	Definition: Specifies the ID of the health check configured for the backend server group. Range: N/A

Parameter	Type	Description
id	String	Definition: Specifies the backend server group ID. Range: N/A
lb_algorithm	String	Definition: Specifies the load balancing algorithm used by the load balancer to route requests to backend servers in the associated backend server group. Range: • ROUND_ROBIN: weighted round robin • LEAST_CONNECTIONS: weighted least connections • SOURCE_IP: source IP hash • QUIC_CID: connection ID
listeners	Array of ListenerRef objects	Definition: Specifies the IDs of the listeners with which the backend server group is associated.
loadbalancers	Array of LoadBalancerRef objects	Definition: Specifies the IDs of the load balancers with which the backend server group is associated.
members	Array of MemberRef objects	Definition: Specifies the IDs of backend servers in the backend server group.
name	String	Definition: Specifies the backend server group name. Range: N/A
project_id	String	Definition: Specifies the project ID of the backend server group. Range: N/A
protocol	String	Definition: Specifies the protocol used by the backend server group to receive requests from the load balancer. Constraints: N/A Range: The value can be TCP , UDP , TLS , HTTP , HTTPS , GRPC , or QUIC . Default value: N/A
session_persistence	SessionPersistence object	Definition: Specifies the sticky session.

Parameter	Type	Description
ip_version	String	Definition: Specifies the IP address version supported by the backend server group. 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	Definition: 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.
member_deletion_protection_enable	Boolean	Definition: Whether to enable removal protection for the backend server. Once the option is enabled, backend servers cannot be removed from the backend server group. Range: false (disable this option) or true (enable this option). NOTE Disable deletion protection or removal protection for your resources before deregistering your account.
created_at	String	Definition: Specifies the creation time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format. Note: This parameter 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	Definition: Specifies the update time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format. Note: This parameter 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	Definition: Specifies the ID of the VPC where the backend server group works. Range: N/A
type	String	Definition: Specifies the backend server group type. Range: • 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	Definition: Specifies the protection status. Range: • nonProtection: The resource is not protected. • consoleProtection: Modification is not allowed on the console.
protection_reason	String	Definition: Specifies why modification protection is enabled. Range: The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).

Parameter	Type	Description
any_port_enable	Boolean	Definition: 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 . Constraints: This option is available only for TCP, UDP, or QUIC backend server groups.
connection_drain	ConnectionDrain object	Definition: Specifies the configurations of deregistration delay. 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	Definition: Specifies the ID of the enterprise project. Range: • 0: The resource belongs to the default enterprise project. • A string in UUID format indicates a non-default enterprise project.
pool_health	PoolHealth object	Definition: Specifies the configurations of the pool health feature.
public_border_group	String	Definition: Specifies the public border group. Range: • center: public border group of the central site • Edge site name: public border group of an edge site
quic_cid_hash_strategy	QuicCidHashStrategy object	Definition: Specifies multi-path distribution configuration based on destination connection IDs.

Table 5-395 AzAffinity

Parameter	Type	Description
enable	Boolean	Definition: Specifies whether to enable AZ affinity for the backend server group. If this parameter is set to true, ELB forwards traffic across the backend servers in the same AZ as the load balancer. Constraints: • This parameter is available only for IP, TCP, and UDP backend server groups. • This parameter is not available for backend server groups that are associated with TLS listeners. • If the parameter is set to true, parameter pool_health will be ignored. Range: false (disable this option) or true (enable this option). Default value: N/A

Parameter	Type	Description
az_minimum_healthy_member_percentage	Integer	Definition: Specifies a percentage that is used to determine the health of an AZ. If the percentage of healthy servers in the AZ of the load balancer falls below the specified value, az_unhealthy_fallback_strategy is triggered. az_minimum_healthy_member_percentage shows the percentage of backend servers that are healthy in a backend server group of an AZ. The number of healthy servers is rounded up. For example, in AZ A, if there are three backend servers in the backend server group and az_minimum_healthy_member_percentage is set to 66%, the number of healthy servers is rounded up to 2 ($3 \times 0.66 = 1.98$). If there are fewer than two healthy servers in AZ A, az_unhealthy_fallback_strategy is triggered. If az_minimum_healthy_member_percentage is set to 67%, the number of healthy servers is rounded up to 3 ($3 \times 0.67 = 2.01$). If there are fewer than three healthy servers in AZ A, az_unhealthy_fallback_strategy is triggered. Constraints: • If enable is set to true, az_minimum_healthy_member_percentage and az_minimum_healthy_member_count cannot be set to -1 at the same time. • If enable is set to true, either az_minimum_healthy_member_percentage or az_minimum_healthy_member_count must be set to -1. Range: an integer ranging from -1 to 100. An integer from 0 to 100 indicates the percentage of healthy servers in the AZ of the load balancer. -1 indicates that az_minimum_healthy_member_count takes effect. Default value: N/A

Parameter	Type	Description
az_minimum_healthy_member_count	Integer	Definition: Specifies a number that is used to determine the health of an AZ. If the number of healthy servers in the AZ of the load balancer falls below the specified value, az_unhealthy_fallback_strategy is triggered. az_minimum_healthy_member_count shows the number of healthy servers in a backend server group of an AZ. Constraints: • If enable is set to true, az_minimum_healthy_member_percentage and az_minimum_healthy_member_count cannot be set to -1 at the same time. • If enable is set to true, either az_minimum_healthy_member_percentage or az_minimum_healthy_member_count must be set to -1. Range: an integer ranging from -1 to 10000. An integer from 0 to 10000 indicates the number of healthy servers in the AZ of the load balancer. -1 indicates that az_minimum_healthy_member_percentage takes effect. Default value: N/A

Parameter	Type	Description
az_unhealthy_fall_back_strategy	String	Definition: Specifies how traffic will be distributed across backend servers in an AZ if the percentage or number of healthy servers in the AZ of the load balancer falls below the specified value. Range: • forward_to_all_member_of_local_az: forwards requests across all backend servers in the same AZ as the load balancer, even if some servers are unhealthy. • forward_to_healthy_member_of_remote_az: forwards requests across healthy backend servers in different AZs from the load balancer. • forward_to_all_healthy_member: forwards requests across healthy backend servers in all AZs. • forward_to_all_member: forwards requests across all backend servers in all AZs, even if some servers are unhealthy. Constraints: N/A Default value: forward_to_all_member_of_local_az

Table 5-396 ListenerRef

Parameter	Type	Description
id	String	Definition: Specifies the listener ID. Range: N/A

Table 5-397 LoadBalancerRef

Parameter	Type	Description
id	String	Definition: Specifies the load balancer ID. Range: N/A

Table 5-398 MemberRef

Parameter	Type	Description
id	String	Specifies the backend server ID. Range: N/A

Table 5-399 SessionPersistence

Parameter	Type	Description
cookie_name	String	Definition: Specifies the cookie name. Range: The value can contain a maximum of 1,024 characters.
type	String	Definition: Specifies the sticky session type. Range: SOURCE_IP , HTTP_COOKIE , or APP_COOKIE .
persistence_timeout	Integer	Definition: Specifies the stickiness duration, in minutes. This parameter will not take effect when type is set to APP_COOKIE . Range: - 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	Definition: Specifies whether to enable slow start. Range: true: This option will be enabled. false: This option will be disabled.
duration	Integer	Definition: Specifies the slow start duration, in seconds. Range: 30 to 1200, in seconds.

Table 5-401 ConnectionDrain

Parameter	Type	Description
enable	Boolean	Definition: Specifies whether to enable connection_drain . Constraints: N/A Range: The value can be true (enable this option) or false (disable this option). Default value: N/A
timeout	Integer	Definition: Specifies the deregistration delay timeout, in seconds. Constraints: N/A Range: 10 to 4000, in seconds. Constraints: N/A

Table 5-402 PoolHealth

Parameter	Type	Description
minimum_healthy_member_count	Integer	Definition: Specifies the number of healthy backend servers below which the backend server group is considered as unhealthy. Range: • 0 (default): pool_health does not take effect. • 1: pool_health takes effect.

Table 5-403 QuicCidHashStrategy

Parameter	Type	Description
len	Integer	Definition: Specifies the length of the hash factor in the connection ID. Constraints: This parameter is valid only when the load balancing algorithm is QUIC_CID . Range: 1 to 20 Default value: 3

Parameter	Type	Description
offset	Integer	Definition: Specifies the start position in the connection ID as the hash factor. Constraints: This parameter is valid only when the load balancing algorithm is QUIC_CID . 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
},
"az_affinity" : {
  "enable" : true,
  "az_minimum_healthy_member_percentage" : -1,
  "az_minimum_healthy_member_count" : 10000,
  "az_unhealthy_fallback_strategy" : "forward_to_all_member_of_local_az"
}
},
"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.ElClientBuilder().
        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 5-404 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
pool_id	Yes	String	Definition: Specifies the backend server group ID. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-405 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-406 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
pool	Pool object	Definition: Specifies the backend server group.

Table 5-407 Pool

Parameter	Type	Description
admin_state_up	Boolean	Definition: Specifies the administrative status of the backend server group. The value can only be true . Range: true (enabled)
az_affinity	AzAffinity object	Definition: Specifies how AZ affinity is configured for the backend server group.
description	String	Definition: Provides supplementary information about the backend server group. Range: N/A
healthmonitor_id	String	Definition: Specifies the ID of the health check configured for the backend server group. Range: N/A
id	String	Definition: Specifies the backend server group ID. Range: N/A

Parameter	Type	Description
lb_algorithm	String	Definition: Specifies the load balancing algorithm used by the load balancer to route requests to backend servers in the associated backend server group. Range: • ROUND_ROBIN: weighted round robin • LEAST_CONNECTIONS: weighted least connections • SOURCE_IP: source IP hash • QUIC_CID: connection ID
listeners	Array of ListenerRef objects	Definition: Specifies the IDs of the listeners with which the backend server group is associated.
loadbalancers	Array of LoadBalancerRef objects	Definition: Specifies the IDs of the load balancers with which the backend server group is associated.
members	Array of MemberRef objects	Definition: Specifies the IDs of backend servers in the backend server group.
name	String	Definition: Specifies the backend server group name. Range: N/A
project_id	String	Definition: Specifies the project ID of the backend server group. Range: N/A
protocol	String	Definition: Specifies the protocol used by the backend server group to receive requests from the load balancer. Constraints: N/A Range: The value can be TCP , UDP , TLS , HTTP , HTTPS , GRPC , or QUIC . Default value: N/A
session_persistence	SessionPersistence object	Definition: Specifies the sticky session.

Parameter	Type	Description
ip_version	String	Definition: Specifies the IP address version supported by the backend server group. 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	Definition: 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.
member_deletion_protection_enable	Boolean	Definition: Whether to enable removal protection for the backend server. Once the option is enabled, backend servers cannot be removed from the backend server group. Range: false (disable this option) or true (enable this option). NOTE Disable deletion protection or removal protection for your resources before deregistering your account.
created_at	String	Definition: Specifies the creation time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format. Note: This parameter 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	Definition: Specifies the update time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format. Note: This parameter 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	Definition: Specifies the ID of the VPC where the backend server group works. Range: N/A
type	String	Definition: Specifies the backend server group type. Range: • 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	Definition: Specifies the protection status. Range: • nonProtection: The resource is not protected. • consoleProtection: Modification is not allowed on the console.
protection_reason	String	Definition: Specifies why modification protection is enabled. Range: The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).

Parameter	Type	Description
any_port_enable	Boolean	Definition: 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 . Constraints: This option is available only for TCP, UDP, or QUIC backend server groups.
connection_drain	ConnectionDrain object	Definition: Specifies the configurations of deregistration delay. 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	Definition: Specifies the ID of the enterprise project. Range: • 0: The resource belongs to the default enterprise project. • A string in UUID format indicates a non-default enterprise project.
pool_health	PoolHealth object	Definition: Specifies the configurations of the pool health feature.
public_border_group	String	Definition: Specifies the public border group. Range: • center: public border group of the central site • Edge site name: public border group of an edge site
quic_cid_hash_strategy	QuicCidHashStrategy object	Definition: Specifies multi-path distribution configuration based on destination connection IDs.

Table 5-408 AzAffinity

Parameter	Type	Description
enable	Boolean	Definition: Specifies whether to enable AZ affinity for the backend server group. If this parameter is set to true, ELB forwards traffic across the backend servers in the same AZ as the load balancer. Constraints: • This parameter is available only for IP, TCP, and UDP backend server groups. • This parameter is not available for backend server groups that are associated with TLS listeners. • If the parameter is set to true, parameter pool_health will be ignored. Range: false (disable this option) or true (enable this option). Default value: N/A

Parameter	Type	Description
az_minimum_healthy_member_percentage	Integer	Definition: Specifies a percentage that is used to determine the health of an AZ. If the percentage of healthy servers in the AZ of the load balancer falls below the specified value, az_unhealthy_fallback_strategy is triggered. az_minimum_healthy_member_percentage shows the percentage of backend servers that are healthy in a backend server group of an AZ. The number of healthy servers is rounded up. For example, in AZ A, if there are three backend servers in the backend server group and az_minimum_healthy_member_percentage is set to 66%, the number of healthy servers is rounded up to 2 ($3 \times 0.66 = 1.98$). If there are fewer than two healthy servers in AZ A, az_unhealthy_fallback_strategy is triggered. If az_minimum_healthy_member_percentage is set to 67%, the number of healthy servers is rounded up to 3 ($3 \times 0.67 = 2.01$). If there are fewer than three healthy servers in AZ A, az_unhealthy_fallback_strategy is triggered. Constraints: • If enable is set to true, az_minimum_healthy_member_percentage and az_minimum_healthy_member_count cannot be set to -1 at the same time. • If enable is set to true, either az_minimum_healthy_member_percentage or az_minimum_healthy_member_count must be set to -1. Range: an integer ranging from -1 to 100. An integer from 0 to 100 indicates the percentage of healthy servers in the AZ of the load balancer. -1 indicates that az_minimum_healthy_member_count takes effect. Default value: N/A

Parameter	Type	Description
az_minimum_healthy_member_count	Integer	Definition: Specifies a number that is used to determine the health of an AZ. If the number of healthy servers in the AZ of the load balancer falls below the specified value, az_unhealthy_fallback_strategy is triggered. az_minimum_healthy_member_count shows the number of healthy servers in a backend server group of an AZ. Constraints: • If enable is set to true, az_minimum_healthy_member_percentage and az_minimum_healthy_member_count cannot be set to -1 at the same time. • If enable is set to true, either az_minimum_healthy_member_percentage or az_minimum_healthy_member_count must be set to -1. Range: an integer ranging from -1 to 10000. An integer from 0 to 10000 indicates the number of healthy servers in the AZ of the load balancer. -1 indicates that az_minimum_healthy_member_percentage takes effect. Default value: N/A

Parameter	Type	Description
az_unhealthy_fall_back_strategy	String	Definition: Specifies how traffic will be distributed across backend servers in an AZ if the percentage or number of healthy servers in the AZ of the load balancer falls below the specified value. Range: • forward_to_all_member_of_local_az: forwards requests across all backend servers in the same AZ as the load balancer, even if some servers are unhealthy. • forward_to_healthy_member_of_remote_az: forwards requests across healthy backend servers in different AZs from the load balancer. • forward_to_all_healthy_member: forwards requests across healthy backend servers in all AZs. • forward_to_all_member: forwards requests across all backend servers in all AZs, even if some servers are unhealthy. Constraints: N/A Default value: forward_to_all_member_of_local_az

Table 5-409 ListenerRef

Parameter	Type	Description
id	String	Definition: Specifies the listener ID. Range: N/A

Table 5-410 LoadBalancerRef

Parameter	Type	Description
id	String	Definition: Specifies the load balancer ID. Range: N/A

Table 5-411 MemberRef

Parameter	Type	Description
id	String	Specifies the backend server ID. Range: N/A

Table 5-412 SessionPersistence

Parameter	Type	Description
cookie_name	String	Definition: Specifies the cookie name. Range: The value can contain a maximum of 1,024 characters.
type	String	Definition: Specifies the sticky session type. Range: SOURCE_IP , HTTP_COOKIE , or APP_COOKIE .
persistence_timeout	Integer	Definition: Specifies the stickiness duration, in minutes. This parameter will not take effect when type is set to APP_COOKIE . Range: - 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 5-413 SlowStart

Parameter	Type	Description
enable	Boolean	Definition: Specifies whether to enable slow start. Range: true: This option will be enabled. false: This option will be disabled.
duration	Integer	Definition: Specifies the slow start duration, in seconds. Range: 30 to 1200, in seconds.

Table 5-414 ConnectionDrain

Parameter	Type	Description
enable	Boolean	Definition: Specifies whether to enable connection_drain . Constraints: N/A Range: The value can be true (enable this option) or false (disable this option). Default value: N/A
timeout	Integer	Definition: Specifies the deregistration delay timeout, in seconds. Constraints: N/A Range: 10 to 4000, in seconds. Constraints: N/A

Table 5-415 PoolHealth

Parameter	Type	Description
minimum_healthy_member_count	Integer	Definition: Specifies the number of healthy backend servers below which the backend server group is considered as unhealthy. Range: • 0 (default): pool_health does not take effect. • 1: pool_health takes effect.

Table 5-416 QuicCidHashStrategy

Parameter	Type	Description
len	Integer	Definition: Specifies the length of the hash factor in the connection ID. Constraints: This parameter is valid only when the load balancing algorithm is QUIC_CID . Range: 1 to 20 Default value: 3

Parameter	Type	Description
offset	Integer	Definition: Specifies the start position in the connection ID as the hash factor. Constraints: This parameter is valid only when the load balancing algorithm is QUIC_CID . 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
    },
    "az_affinity" : {
      "enable" : "true",
      "az_minimum_healthy_member_percentage" : -1,
      "az_minimum_healthy_member_count" : 10000,
      "az_unhealthy_fallback_strategy" : "forward_to_all_member_of_local_az"
    }
  },
}
```

```
"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.getErrMsg());
        }
    }
}
```

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 5-417 Path Parameters

Parameter	Mandatory	Type	Description
pool_id	Yes	String	Definition: Specifies the backend server group ID. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-418 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-419 Request body parameters

Parameter	Mandatory	Type	Description
pool	Yes	UpdatePoolOption object	Definition: Specifies the request parameters for updating a backend server group. Constraints: N/A

Table 5-420 UpdatePoolOption

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Definition: Specifies the administrative status of the backend server group. Constraints: The value can only be true . Range: true (enabled) Default value: N/A
description	No	String	Definition: Specifies supplementary information about the backend server group. Constraints: N/A Range: N/A Default value: N/A
lb_algorithm	No	String	Definition: Specifies the load balancing algorithm used by the load balancer to route requests to backend servers in the associated backend server group. Constraints: • If the value is SOURCE_IP or QUIC_CID, the weights of backend servers in the backend server group are invalid. • QUIC_CID is available only when the protocol of the backend server group is QUIC. Range: • ROUND_ROBIN: weighted round robin • LEAST_CONNECTIONS: weighted least connections • SOURCE_IP: source IP hash • QUIC_CID: connection ID Default value: N/A

Parameter	Mandatory	Type	Description
name	No	String	Definition: Specifies the backend server group name. Constraints: N/A Range: N/A Default value: N/A
session_persistence	No	UpdatePoolSessionPersistenceOption object	Definition: Specifies the sticky session. Constraints: Slow start and sticky session cannot be enabled at the same time. If both are enabled, sticky session will be invalid.
slow_start	No	UpdatePoolSlowStartOption object	Definition: 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. Constraints: • This parameter is valid only when the backend server group protocol is HTTP, HTTPS, or GRPC. For other protocols, an error will be reported. • Slow start and sticky session cannot be enabled at the same time. If both are enabled, sticky session will be invalid.

Parameter	Mandatory	Type	Description
member_deletion_protection_enable	No	Boolean	Definition: Whether to enable removal protection for the backend server. Once the option is enabled, backend servers cannot be removed from the backend server group. Constraints: Once the option is enabled, an error will be returned when the following APIs are called to: • Delete a load balancer and its associated resources (DELETE /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}/force-elb). • Delete a load balancer and its associated EIPs (POST /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}/delete-cascade). • Delete a listener and its associated resources (DELETE /v3/{project_id}/elb/listeners/{listener_id}/force). • Delete a backend server group and its associated resources (DELETE /v3/{project_id}/elb/pools/{pool_id}/delete-cascade). • Remove a backend server (DELETE /v3/{project_id}/elb/pools/{pool_id}/members/{member_id}). • Remove backend servers in batches (POST /v3/{project_id}/elb/pools/{pool_id}/members/batch-delete). Range: false (disable this option) or true (enable this option).

Parameter	Mandatory	Type	Description
			Default value: false NOTE Disable deletion protection or removal protection for your resources before deregistering your account.
vpc_id	No	String	Definition: Specifies the ID of the VPC where the backend server group works. Constraints: This parameter can be updated only when vpc_id is left blank. Range: N/A Default value: N/A
type	No	String	Definition: Specifies the type of the backend server group. Constraints: • This parameter can be updated only when type is left blank. • 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. Range: N/A Default value: N/A
protection_status	No	String	Definition: Specifies the protection status. Constraints: N/A Value options: • nonProtection: The resource is not protected. • consoleProtection: Modification is not allowed on the console. Default value: N/A

Parameter	Mandatory	Type	Description
protection_reason	No	String	Definition: Specifies why modification protection is enabled. Constraints: This parameter is valid only when protection_status is set to consoleProtection . Range: The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>). Default value: N/A
any_port_enable	No	Boolean	Definition: 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 . Constraints: This option is available only for TCP, UDP, or QUIC backend server groups. Range: false (disable this option) or true (enable this option). Default value: false

Parameter	Mandatory	Type	Description
connection_drain	No	ConnectionDrain object	Definition: Specifies the configurations of deregistration delay. 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. Constraints: This parameter is only available for TCP, UDP, and QUIC backend server groups and TCP and UDP listeners.
pool_health	No	PoolHealth object	Definition: Specifies the configurations of the pool health feature. Constraints: N/A
quic_cid_hash_strategy	No	QuicCidHashStrategy object	Definition: Specifies multi-path distribution configuration based on destination connection IDs. Constraints: N/A
az_affinity	No	UpdateAzAffinity object	Definition: Specifies how AZ affinity is configured for the backend server group. Constraints: N/A

Table 5-421 UpdatePoolSessionPersistenceOption

Parameter	Mandatory	Type	Description
cookie_name	No	String	Definition: Specifies the cookie name. Constraints: This parameter takes effect only when type is set to APP_COOKIE. Otherwise, an error will be returned. Range: The value can contain a maximum of 1,024 characters. Default value: N/A
type	No	String	Definition: Specifies the sticky session type. 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, only HTTP_COOKIE and APP_COOKIE take effect. - If the backend server group's protocol is QUIC, session_persistence must be set to true and type set to SOURCE_IP. Range: SOURCE_IP , HTTP_COOKIE , or APP_COOKIE . Default value: N/A

Parameter	Mandatory	Type	Description
persistence_timeout	No	Integer	Definition: Specifies the stickiness duration, in minutes. Constraints: This parameter will not take effect when type is set to APP_COOKIE . Range: • 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. Default value: N/A

Table 5-422 UpdatePoolSlowStartOption

Parameter	Mandatory	Type	Description
enable	No	Boolean	Definition: Specifies whether to enable slow start. Constraints: N/A • true: Enable slow start. • false: Disable slow start. Default value: N/A
duration	No	Integer	Definition: Specifies the slow start duration, in seconds. Constraints: N/A Range: 30 to 1200 Default value: N/A

Table 5-423 ConnectionDrain

Parameter	Mandatory	Type	Description
enable	No	Boolean	Definition: Specifies whether to enable connection_drain . Constraints: N/A Range: The value can be true (enable this option) or false (disable this option). Default value: N/A
timeout	No	Integer	Definition: Specifies the deregistration delay timeout, in seconds. Constraints: N/A Range: 10 to 4000, in seconds. Constraints: N/A

Table 5-424 PoolHealth

Parameter	Mandatory	Type	Description
minimum_healthy_member_count	No	Integer	Definition: Specifies the number of healthy backend servers below which the backend server group is considered as unhealthy. Range: • 0 (default): pool_health does not take effect. • 1: pool_health takes effect.

Table 5-425 QuicCidHashStrategy

Parameter	Mandatory	Type	Description
len	Yes	Integer	Definition: Specifies the length of the hash factor in the connection ID. Constraints: This parameter is valid only when the load balancing algorithm is QUIC_CID . Range: 1 to 20 Default value: 3

Parameter	Mandatory	Type	Description
offset	Yes	Integer	Definition: Specifies the start position in the connection ID as the hash factor. Constraints: This parameter is valid only when the load balancing algorithm is QUIC_CID . Range: 0 to 19 Default value: 1

Table 5-426 UpdateAzAffinity

Parameter	Mandatory	Type	Description
enable	No	Boolean	Definition: Specifies whether to enable AZ affinity for the backend server group. If this parameter is set to true , ELB forwards traffic across the backend servers in the same AZ as the load balancer. Constraints: • AZ affinity cannot be enabled for a backend server group that has IP as backend servers whose availability_zone is not specified. • AZ affinity cannot be enabled if the backend server is bound to a TLS listener. • This parameter is available for backend server groups that are associated with IP, UDP, and TCP listeners. • If the parameter is set to true, parameter pool_health will be ignored. Range: false (disable this option) or true (enable this option). Default value: N/A

Parameter	Mandatory	Type	Description
az_minimum_healthy_member_percentage	No	Integer	Definition: Specifies a percentage that is used to determine the health of an AZ. If the percentage of healthy servers in the AZ of the load balancer falls below the specified value, az_unhealthy_fallback_strategy is triggered. az_minimum_healthy_member_percentage shows the percentage of backend servers that are healthy in a backend server group of an AZ. The number of healthy servers is rounded up. For example, in AZ A, if there are three backend servers in the backend server group and az_minimum_healthy_member_percentage is set to 66%, the number of healthy servers is rounded up to 2 ($3 \times 0.66 = 1.98$). If there are fewer than two healthy servers in AZ A, az_unhealthy_fallback_strategy is triggered. If az_minimum_healthy_member_percentage is set to 67%, the number of healthy servers is rounded up to 3 ($3 \times 0.67 = 2.01$). If there are fewer than three healthy servers in AZ A, az_unhealthy_fallback_strategy is triggered. Constraints: • If enable is set to true, az_minimum_healthy_member_percentage and az_minimum_healthy_member_count cannot be set to -1 at the same time. • If enable is set to true, either az_minimum_healthy_member_percentage or az_minimum_healthy_member_count must be set to -1.

Parameter	Mandatory	Type	Description
			Range: an integer ranging from -1 to 100. An integer from 0 to 100 indicates the percentage of healthy servers in the AZ of the load balancer. -1 indicates that az_minimum_healthy_member_count takes effect. Default value: N/A
az_minimum_healthy_member_count	No	Integer	Definition: Specifies a number that is used to determine the health of an AZ. If the number of healthy servers in the AZ of the load balancer falls below the specified value, az_unhealthy_fallback_strategy is triggered. az_minimum_healthy_member_count shows the number of healthy servers in a backend server group of an AZ. Constraints: • If enable is set to true, az_minimum_healthy_member_percentage and az_minimum_healthy_member_count cannot be set to -1 at the same time. • If enable is set to true, either az_minimum_healthy_member_percentage or az_minimum_healthy_member_count must be set to -1. Range: an integer ranging from -1 to 10000. An integer from 0 to 10000 indicates the number of healthy servers in the AZ of the load balancer. -1 indicates that az_minimum_healthy_member_percentage takes effect. Default value: N/A

Parameter	Mandatory	Type	Description
az_unhealthy_fallback_strategy	No	String	Definition: Specifies how traffic will be distributed across backend servers in an AZ if the percentage or number of healthy servers in the AZ of the load balancer falls below the specified value. Range: • forward_to_all_member_of_local_az: forwards requests across all backend servers in the same AZ as the load balancer, even if some servers are unhealthy. • forward_to_healthy_member_of_remote_az: forwards requests across healthy backend servers in different AZs from the load balancer. • forward_to_all_healthy_member: forwards requests across healthy backend servers in all AZs. • forward_to_all_member: forwards requests across all backend servers in all AZs, even if some servers are unhealthy. Constraints: N/A Default value: forward_to_all_member_of_local_az

Response Parameters

Status code: 200

Table 5-427 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
pool	Pool object	Definition: Specifies the response parameters for updating a backend server group.

Table 5-428 Pool

Parameter	Type	Description
admin_state_up	Boolean	Definition: Specifies the administrative status of the backend server group. The value can only be true . Range: true (enabled)
az_affinity	AzAffinity object	Definition: Specifies how AZ affinity is configured for the backend server group.
description	String	Definition: Provides supplementary information about the backend server group. Range: N/A
healthmonitor_id	String	Definition: Specifies the ID of the health check configured for the backend server group. Range: N/A
id	String	Definition: Specifies the backend server group ID. Range: N/A

Parameter	Type	Description
lb_algorithm	String	Definition: Specifies the load balancing algorithm used by the load balancer to route requests to backend servers in the associated backend server group. Range: • ROUND_ROBIN: weighted round robin • LEAST_CONNECTIONS: weighted least connections • SOURCE_IP: source IP hash • QUIC_CID: connection ID
listeners	Array of ListenerRef objects	Definition: Specifies the IDs of the listeners with which the backend server group is associated.
loadbalancers	Array of LoadBalancerRef objects	Definition: Specifies the IDs of the load balancers with which the backend server group is associated.
members	Array of MemberRef objects	Definition: Specifies the IDs of backend servers in the backend server group.
name	String	Definition: Specifies the backend server group name. Range: N/A
project_id	String	Definition: Specifies the project ID of the backend server group. Range: N/A
protocol	String	Definition: Specifies the protocol used by the backend server group to receive requests from the load balancer. Constraints: N/A Range: The value can be TCP , UDP , TLS , HTTP , HTTPS , GRPC , or QUIC . Default value: N/A
session_persistence	SessionPersistence object	Definition: Specifies the sticky session.

Parameter	Type	Description
ip_version	String	Definition: Specifies the IP address version supported by the backend server group. 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	Definition: 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.
member_deletion_protection_enable	Boolean	Definition: Whether to enable removal protection for the backend server. Once the option is enabled, backend servers cannot be removed from the backend server group. Range: false (disable this option) or true (enable this option). NOTE Disable deletion protection or removal protection for your resources before deregistering your account.
created_at	String	Definition: Specifies the creation time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format. Note: This parameter 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	Definition: Specifies the update time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format. Note: This parameter 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	Definition: Specifies the ID of the VPC where the backend server group works. Range: N/A
type	String	Definition: Specifies the backend server group type. Range: • 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	Definition: Specifies the protection status. Range: • nonProtection: The resource is not protected. • consoleProtection: Modification is not allowed on the console.
protection_reason	String	Definition: Specifies why modification protection is enabled. Range: The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).

Parameter	Type	Description
any_port_enable	Boolean	Definition: 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 . Constraints: This option is available only for TCP, UDP, or QUIC backend server groups.
connection_drain	ConnectionDrain object	Definition: Specifies the configurations of deregistration delay. 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	Definition: Specifies the ID of the enterprise project. Range: • 0: The resource belongs to the default enterprise project. • A string in UUID format indicates a non-default enterprise project.
pool_health	PoolHealth object	Definition: Specifies the configurations of the pool health feature.
public_border_group	String	Definition: Specifies the public border group. Range: • center: public border group of the central site • Edge site name: public border group of an edge site
quic_cid_hash_strategy	QuicCidHashStrategy object	Definition: Specifies multi-path distribution configuration based on destination connection IDs.

Table 5-429 AzAffinity

Parameter	Type	Description
enable	Boolean	Definition: Specifies whether to enable AZ affinity for the backend server group. If this parameter is set to true, ELB forwards traffic across the backend servers in the same AZ as the load balancer. Constraints: • This parameter is available only for IP, TCP, and UDP backend server groups. • This parameter is not available for backend server groups that are associated with TLS listeners. • If the parameter is set to true, parameter pool_health will be ignored. Range: false (disable this option) or true (enable this option). Default value: N/A

Parameter	Type	Description
az_minimum_healthy_member_percentage	Integer	Definition: Specifies a percentage that is used to determine the health of an AZ. If the percentage of healthy servers in the AZ of the load balancer falls below the specified value, az_unhealthy_fallback_strategy is triggered. az_minimum_healthy_member_percentage shows the percentage of backend servers that are healthy in a backend server group of an AZ. The number of healthy servers is rounded up. For example, in AZ A, if there are three backend servers in the backend server group and az_minimum_healthy_member_percentage is set to 66%, the number of healthy servers is rounded up to 2 ($3 \times 0.66 = 1.98$). If there are fewer than two healthy servers in AZ A, az_unhealthy_fallback_strategy is triggered. If az_minimum_healthy_member_percentage is set to 67%, the number of healthy servers is rounded up to 3 ($3 \times 0.67 = 2.01$). If there are fewer than three healthy servers in AZ A, az_unhealthy_fallback_strategy is triggered. Constraints: • If enable is set to true, az_minimum_healthy_member_percentage and az_minimum_healthy_member_count cannot be set to -1 at the same time. • If enable is set to true, either az_minimum_healthy_member_percentage or az_minimum_healthy_member_count must be set to -1. Range: an integer ranging from -1 to 100. An integer from 0 to 100 indicates the percentage of healthy servers in the AZ of the load balancer. -1 indicates that az_minimum_healthy_member_count takes effect. Default value: N/A

Parameter	Type	Description
az_minimum_healthy_member_count	Integer	Definition: Specifies a number that is used to determine the health of an AZ. If the number of healthy servers in the AZ of the load balancer falls below the specified value, az_unhealthy_fallback_strategy is triggered. az_minimum_healthy_member_count shows the number of healthy servers in a backend server group of an AZ. Constraints: • If enable is set to true, az_minimum_healthy_member_percentage and az_minimum_healthy_member_count cannot be set to -1 at the same time. • If enable is set to true, either az_minimum_healthy_member_percentage or az_minimum_healthy_member_count must be set to -1. Range: an integer ranging from -1 to 10000. An integer from 0 to 10000 indicates the number of healthy servers in the AZ of the load balancer. -1 indicates that az_minimum_healthy_member_percentage takes effect. Default value: N/A

Parameter	Type	Description
az_unhealthy_fall_back_strategy	String	Definition: Specifies how traffic will be distributed across backend servers in an AZ if the percentage or number of healthy servers in the AZ of the load balancer falls below the specified value. Range: • forward_to_all_member_of_local_az: forwards requests across all backend servers in the same AZ as the load balancer, even if some servers are unhealthy. • forward_to_healthy_member_of_remote_az: forwards requests across healthy backend servers in different AZs from the load balancer. • forward_to_all_healthy_member: forwards requests across healthy backend servers in all AZs. • forward_to_all_member: forwards requests across all backend servers in all AZs, even if some servers are unhealthy. Constraints: N/A Default value: forward_to_all_member_of_local_az

Table 5-430 ListenerRef

Parameter	Type	Description
id	String	Definition: Specifies the listener ID. Range: N/A

Table 5-431 LoadBalancerRef

Parameter	Type	Description
id	String	Definition: Specifies the load balancer ID. Range: N/A

Table 5-432 MemberRef

Parameter	Type	Description
id	String	Specifies the backend server ID. Range: N/A

Table 5-433 SessionPersistence

Parameter	Type	Description
cookie_name	String	Definition: Specifies the cookie name. Range: The value can contain a maximum of 1,024 characters.
type	String	Definition: Specifies the sticky session type. Range: SOURCE_IP, HTTP_COOKIE, or APP_COOKIE.
persistence_timeout	Integer	Definition: Specifies the stickiness duration, in minutes. This parameter will not take effect when type is set to APP_COOKIE. Range: - 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 5-434 SlowStart

Parameter	Type	Description
enable	Boolean	Definition: Specifies whether to enable slow start. Range: true: This option will be enabled. false: This option will be disabled.
duration	Integer	Definition: Specifies the slow start duration, in seconds. Range: 30 to 1200, in seconds.

Table 5-435 ConnectionDrain

Parameter	Type	Description
enable	Boolean	Definition: Specifies whether to enable connection_drain . Constraints: N/A Range: The value can be true (enable this option) or false (disable this option). Default value: N/A
timeout	Integer	Definition: Specifies the deregistration delay timeout, in seconds. Constraints: N/A Range: 10 to 4000, in seconds. Constraints: N/A

Table 5-436 PoolHealth

Parameter	Type	Description
minimum_healthy_member_count	Integer	Definition: Specifies the number of healthy backend servers below which the backend server group is considered as unhealthy. Range: • 0 (default): pool_health does not take effect. • 1: pool_health takes effect.

Table 5-437 QuicCidHashStrategy

Parameter	Type	Description
len	Integer	Definition: Specifies the length of the hash factor in the connection ID. Constraints: This parameter is valid only when the load balancing algorithm is QUIC_CID . Range: 1 to 20 Default value: 3

Parameter	Type	Description
offset	Integer	Definition: Specifies the start position in the connection ID as the hash factor. Constraints: This parameter is valid only when the load balancing algorithm is QUIC_CID . 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.getErrMsg());  
        }  
    }  
}
```

```
}  
}  
}
```

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 5-438 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
pool_id	Yes	String	Definition: Specifies the backend server group ID. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-439 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 204

Successful request.

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 huaweicloudskelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskelb.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 5-440 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
pool_id	Yes	String	Definition: Specifies the backend server group ID. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-441 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 204

Successful request.

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 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	Successful request.

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 5-442 Path Parameters

Parameter	Mandatory	Type	Description
pool_id	Yes	String	Definition: Specifies the backend server group ID. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-443 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-444 Request body parameters

Parameter	Mandatory	Type	Description
member	Yes	CreateMemberOption object	Definition: Specifies the backend server. Constraints: N/A

Table 5-445 CreateMemberOption

Parameter	Mandatory	Type	Description
address	Yes	String	Definition: Specifies the IP address of the backend server. Constraints: • If subnet_cidr_id is left blank, IP as backend servers will be added. In this case, the IP address must be an IPv4 address. • If subnet_cidr_id is not left blank, ECSs will be added as backend servers. It must be in the subnet specified by subnet_cidr_id. Range: N/A Default value: N/A
admin_state_up	No	Boolean	Definition: Specifies the administrative status of the backend server. Constraints: Although this parameter can be used in the APIs for creating and updating backend servers, its actual value depends on whether ECSs exist. Range: If ECSs exist, the value is true . Otherwise, the value is false . Default value: N/A
name	No	String	Definition: 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. Constraints: N/A Range: N/A Default value: N/A
project_id	No	String	Definition: Specifies the project ID of the backend server. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
protocol_port	No	Integer	Definition: Specifies the port used by the backend server to receive requests. Constraints: • 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. Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
subnet_cidr_id	No	String	Definition: 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 parameter neutron_subnet_id in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets) to get the IPv4 subnet ID. You can query parameter neutron_network_id in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets) to get the IPv6 subnet ID. Constraints: • 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, indicating that an IP as backend server will be added. 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. Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
weight	No	Integer	Definition: Specifies the weight of the backend server. Requests are routed based on the load balancing algorithm configured for the backend server group and weights of backend servers. 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. Constraints: If lb_algorithm is set to SOURCE_IP or QUIC_CID, this parameter will not take effect. Range: 0 to 100. The default value is 1. Default value: N/A
availability_zone	No	String	Definition: Specifies the AZ of the backend server. Constraints: • This parameter can be only set for IP as backend servers. If AZ affinity is enabled for the backend server group, this parameter must be set to a valid value for IP as backend servers. Range: AZs available for ECSs in the current region. Default value: N/A

Response Parameters

Status code: 201

Table 5-446 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
member	Member object	Definition: Specifies the backend server.

Table 5-447 Member

Parameter	Type	Description
id	String	Definition: Specifies the backend server ID. Range: N/A NOTE The value of this parameter is not the ID of the server but an ID automatically generated for the backend server that is associated with the load balancer.
availability_zone	String	Definition: Specifies the AZ where the backend server is running. Range: N/A
name	String	Definition: Specifies the backend server name. Range: N/A Note: The name is not an ECS name.
project_id	String	Definition: Specifies the project ID of the backend server. Range: N/A
admin_state_up	Boolean	Definition: Specifies the administrative status of the backend server. Range: true or false

Parameter	Type	Description
subnet_cidr_id	String	Definition: 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 parameter neutron_subnet_id in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets) to get the IPv4 subnet ID. You can query parameter neutron_network_id in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets) to get the IPv6 subnet ID. Range: N/A
protocol_port	Integer	Definition: Specifies the port used by the backend server to receive requests. Range: N/A 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	Definition: Specifies the weight of the backend server. Requests are routed based on the load balancing algorithm configured for the backend server group and weights of backend servers. 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. Range: 0 to 100
address	String	Definition: Specifies the IP address of the backend server Range: N/A
ip_version	String	Definition: Specifies the IP address version supported by the backend server. The version depends on the value of address returned by the system. Range: v4 or v6

Parameter	Type	Description
operating_status	String	Definition: Specifies the operating status of the backend server. Range: • NO_MONITOR: No health check is configured for the backend server group to which the backend server belongs. • INITIAL: The backend server is initializing. Health check is configured for the backend server group, but no data has been reported yet. • ONLINE: The backend server is running normally. • OFFLINE: The backend server is detected unhealthy, or the cloud server used as the backend server is stopped or does not exist. • UNKNOWN: The health check has not started yet, or no listener is associated with the backend server group, or the member IP address is not assigned to a cloud service instance (such as ECS, network interface, or supplementary network interface). Multiple statuses can be used for query in the format of <i>operating_status=xxx&operating_status=xxx</i> .
status	Array of MemberStatus objects	Definition: Specifies the health status of the backend server. Range: N/A
reason	MemberHealthCheckFailedReason object	Definition: Specifies why health check fails.
created_at	String	Definition: Specifies the creation time. The value must be a UTC time in the format of <i>yyyy-MM-dd'THH:mm:ss'Z'</i> . Range: N/A Note: This parameter 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	Definition: Specifies the update time. The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Range: N/A Note: This parameter 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	Definition: Specifies the backend server type. Range: • ip: IP as backend servers • instance: ECSs used as backend servers
instance_id	String	Definition: 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. Range: N/A

Table 5-448 MemberStatus

Parameter	Type	Description
listener_id	String	Definition: Specifies the listener ID. Range: N/A
operating_status	String	Definition: Specifies the operating status of the backend server. Range: • 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 ECS used as the backend server is stopped or does not exist.
reason	MemberHealthCheckFailedReason object	Definition: Specifies why the health check fails.

Parameter	Type	Description
created_at	String	Definition: Specifies the creation time. The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Range: N/A
updated_at	String	Definition: Specifies the update time. The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Range: N/A

Table 5-449 MemberHealthCheckFailedReason

Parameter	Type	Description
reason_code	String	Definition: Specifies the code of the health check failures. Range: • 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	Definition: 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 . 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. • 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	Definition: 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 . 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

Successful request.

```
{  
  "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"  
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

- Example 1: Adding 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 CreateMemberSolution {
```

```
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();

    CreateMemberRequest request = new CreateMemberRequest();
    request.withPoolId("{pool_id}");
    CreateMemberRequestBody body = new CreateMemberRequestBody();
    CreateMemberOption memberbody = new CreateMemberOption();
    memberbody.withAddress("120.10.10.16")
        .withName("My member")
        .withProtocolPort(89)
        .withSubnetCidrId("c09f620e-3492-4429-ac15-445d5dd9ca74");
    body.withMember(memberbody);
    request.withBody(body);
    try {
        CreateMemberResponse response = client.createMember(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 IP address as 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 CreateMemberSolution {

    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();
CreateMemberRequest request = new CreateMemberRequest();
request.withPoolId("{pool_id}");
CreateMemberRequestBody body = new CreateMemberRequestBody();
CreateMemberOption memberbody = new CreateMemberOption();
memberbody.withAddress("120.10.10.16")
    .withName("My member")
    .withProtocolPort(89);
body.withMember(memberbody);
request.withBody(body);
try {
    CreateMemberResponse response = client.createMember(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 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 = CreateMemberRequest()
request.pool_id = "{pool_id}"
memberbody = CreateMemberOption(
    address="120.10.10.16",
    name="My member",
    protocol_port=89,
    subnet_cidr_id="c09f620e-3492-4429-ac15-445d5dd9ca74"
)
request.body = CreateMemberRequestBody(
    member=memberbody
)
response = client.create_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)
```

- Example 2: Adding an IP address as 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 = CreateMemberRequest()
        request.pool_id = "{pool_id}"
        memberbody = CreateMemberOption(
            address="120.10.10.16",
            name="My member",
            protocol_port=89
        )
        request.body = CreateMemberRequestBody(
            member=memberbody
        )
        response = client.create_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

- Example 1: Adding 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.ElClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.CreateMemberRequest{}
    request.PoolId = "{pool_id}"
    nameMember := "My member"
    protocolPortMember := int32(89)
    subnetCidrIdMember := "c09f620e-3492-4429-ac15-445d5dd9ca74"
    memberbody := &model.CreateMemberOption{
        Address: "120.10.10.16",
        Name: &nameMember,
        ProtocolPort: &protocolPortMember,
        SubnetCidrId: &subnetCidrIdMember,
    }
    request.Body = &model.CreateMemberRequestBody{
        Member: memberbody,
    }
    response, err := client.CreateMember(request)
    if err == nil {
        fmt.Printf("%+v\n", response)
    } else {
        fmt.Println(err)
    }
}
```

- Example 2: Adding an IP address as 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.ElClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.CreateMemberRequest{}
request.PoolId = "{pool_id}"
nameMember := "My member"
protocolPortMember := int32(89)
memberbody := &model.CreateMemberOption{
    Address: "120.10.10.16",
    Name: &nameMember,
    ProtocolPort: &protocolPortMember,
}
request.Body = &model.CreateMemberRequestBody{
    Member: memberbody,
}
response, err := client.CreateMember(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	Successful request.

Error Codes

See [Error Codes](#).

5.12.2 Querying Backend Servers in a Backend Server Group

Function

This API is used to query all backend servers in a given backend server group.

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 5-450 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
pool_id	Yes	String	Definition: Specifies the backend server group ID. Constraints: N/A Range: N/A Default value: N/A

Table 5-451 Query Parameters

Parameter	Mandatory	Type	Description
marker	No	String	Definition: Specifies the ID of the last record on the previous page. Constraints: • This parameter must be used together with limit. • If the parameter is not specified, only resources on the first page are queried. • This parameter cannot be left blank or set to an invalid ID. Range: N/A Default value: N/A
limit	No	Integer	Definition: Specifies the number of records returned on each page. Constraints: N/A Range: 0 to 2000 Default value: 2000
page_reverse	No	Boolean	Definition: Specifies whether to use reverse query. Constraints: • This parameter must be used together with limit. • If page_reverse is set to true and you want to query the resources on the previous page, set the value of marker to the value of previous_marker. Range: • true: Query resources on the previous page. • false: Query resources on the next page. Default value: false

Parameter	Mandatory	Type	Description
name	No	Array of strings	Definition: Specifies the backend server name. Note: The name is not an ECS name. Multiple names can be used for query in the format of <i>name=xxx&name=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
weight	No	Array of integers	Definition: Specifies the weight of the backend server. Requests are routed based on the load balancing algorithm configured for the backend server group and weights of backend servers. 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 used for query in the format of <i>weight=xxx&weight=xxx</i> . Constraints: N/A Range: 0 to 100 Default value: N/A
admin_state_up	No	Boolean	Definition: Specifies the administrative status of the backend server. Constraints: N/A Range: true or false Default value: N/A

Parameter	Mandatory	Type	Description
subnet_cidr_id	No	Array of strings	Definition: Specifies the ID of the IPv4 or IPv6 subnet where the backend server resides. Multiple IDs can be used for query in the format of <i>subnet_cidr_id=xxx&subnet_cidr_id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
address	No	Array of strings	Definition: Specifies the IPv4 or IPv6 address bound to the backend server. Multiple IP addresses can be used for query in the format of <i>address=xxx&address=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
protocol_port	No	Array of integers	Definition: Specifies the port used by the backend server to receive requests. Multiple ports can be used for query in the format of <i>protocol_port=xxx&protocol_port=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
id	No	Array of strings	Definition: Specifies the backend server ID. Multiple IDs can be used for query in the format of <i>id=xxx&id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
operating_status	No	Array of strings	Definition: Specifies the operating status of the backend server. Multiple operating statuses can be used for query in the format of <i>operating_status=xxx&operating_status=xxx</i>. Constraints: N/A Range: • NO_MONITOR: No health check is configured for the backend server group to which the backend server belongs. • INITIAL: The backend server is initializing. Health check is configured for the backend server group, but no data has been reported yet. • ONLINE: The backend server is running normally. • OFFLINE: The backend server is detected unhealthy, or the cloud server used as the backend server is stopped or does not exist. • UNKNOWN: The health check has not started yet, or no listener is associated with the backend server group, or the member IP address is not assigned to a cloud service instance (such as ECS, network interface, or supplementary network interface). Default value: N/A

Parameter	Mandatory	Type	Description
enterprise_project_id	No	Array of strings	Definition: Specifies the ID of the enterprise project. Multiple values can be used for query in the format of: <i>enterprise_project_id=xxx&enterprise_project_id=xxx.</i> Constraints: • 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. Range: N/A Default value: N/A
ip_version	No	Array of strings	Definition: Specifies the IP version supported by the backend server. Constraints: N/A Range: v4 (IPv4) or v6 (IPv6) Default value: N/A

Parameter	Mandatory	Type	Description
member_type	No	Array of strings	Definition: Specifies the type of the backend server. Multiple values can be used for query in the format of <i>member_type=xxx&member_type=xxx</i> . Constraints: N/A Range: • ip: IP as backend servers • instance: ECSs used as backend servers Default value: N/A
instance_id	No	Array of strings	Definition: 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 used for query in the format of <i>instance_id=xxx&instance_id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
availability_zone	No	Array of strings	Definition: Specifies the backend server AZ. Multiple values can be used for query in the format of <i>availability_zone=xxx&availability_zone=xxx</i> . Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-452 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-453 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
page_info	PageInfo object	Definition: Specifies the pagination information.
members	Array of Member objects	Definition: Specifies the backend servers.

Table 5-454 PageInfo

Parameter	Type	Description
previous_marker	String	Definition: Specifies the ID of the first record in the pagination query result. If page_reverse is set to true , this parameter is used together to query resources on the previous page. Range: N/A
next_marker	String	Definition: Specifies the ID of the last record in the pagination query result. It is usually used to query resources on the next page. Range: N/A

Parameter	Type	Description
current_count	Integer	Definition: Specifies the number of records returned on the current page. Range: N/A

Table 5-455 Member

Parameter	Type	Description
id	String	Definition: Specifies the backend server ID. Range: N/A NOTE The value of this parameter is not the ID of the server but an ID automatically generated for the backend server that is associated with the load balancer.
availability_zone	String	Definition: Specifies the AZ where the backend server is running. Range: N/A
name	String	Definition: Specifies the backend server name. Range: N/A Note: The name is not an ECS name.
project_id	String	Definition: Specifies the project ID of the backend server. Range: N/A
admin_state_up	Boolean	Definition: Specifies the administrative status of the backend server. Range: true or false

Parameter	Type	Description
subnet_cidr_id	String	Definition: 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 parameter neutron_subnet_id in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets) to get the IPv4 subnet ID. You can query parameter neutron_network_id in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets) to get the IPv6 subnet ID. Range: N/A
protocol_port	Integer	Definition: Specifies the port used by the backend server to receive requests. Range: N/A 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	Definition: Specifies the weight of the backend server. Requests are routed based on the load balancing algorithm configured for the backend server group and weights of backend servers. 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. Range: 0 to 100
address	String	Definition: Specifies the IP address of the backend server Range: N/A
ip_version	String	Definition: Specifies the IP address version supported by the backend server. The version depends on the value of address returned by the system. Range: v4 or v6

Parameter	Type	Description
operating_status	String	Definition: Specifies the operating status of the backend server. Range: • NO_MONITOR: No health check is configured for the backend server group to which the backend server belongs. • INITIAL: The backend server is initializing. Health check is configured for the backend server group, but no data has been reported yet. • ONLINE: The backend server is running normally. • OFFLINE: The backend server is detected unhealthy, or the cloud server used as the backend server is stopped or does not exist. • UNKNOWN: The health check has not started yet, or no listener is associated with the backend server group, or the member IP address is not assigned to a cloud service instance (such as ECS, network interface, or supplementary network interface). Multiple statuses can be used for query in the format of <i>operating_status=xxx&operating_status=xxx</i>.
status	Array of MemberStatus objects	Definition: Specifies the health status of the backend server. Range: N/A
reason	MemberHealthCheckFailedReason object	Definition: Specifies why health check fails.
created_at	String	Definition: Specifies the creation time. The value must be a UTC time in the format of <i>yyyy-MM-dd'THH:mm:ss'Z'</i>. Range: N/A Note: This parameter 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	Definition: Specifies the update time. The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Range: N/A Note: This parameter 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	Definition: Specifies the backend server type. Range: • ip: IP as backend servers • instance: ECSs used as backend servers
instance_id	String	Definition: 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. Range: N/A

Table 5-456 MemberStatus

Parameter	Type	Description
listener_id	String	Definition: Specifies the listener ID. Range: N/A
operating_status	String	Definition: Specifies the operating status of the backend server. Range: • 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 ECS used as the backend server is stopped or does not exist.
reason	MemberHealthCheckFailedReason object	Definition: Specifies why the health check fails.

Parameter	Type	Description
created_at	String	Definition: Specifies the creation time. The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Range: N/A
updated_at	String	Definition: Specifies the update time. The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Range: N/A

Table 5-457 MemberHealthCheckFailedReason

Parameter	Type	Description
reason_code	String	Definition: Specifies the code of the health check failures. Range: • 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	Definition: 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 . 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. • 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	Definition: 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 . 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",
    "availability_zone": "az1"
  }, {
    "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",
    "availability_zone": "az2"
  }, {
    "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",
    "availability_zone": "az2"
  } ],
  "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.getErrMsg());
        }
    }
}
```

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 5-458 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
pool_id	Yes	String	Definition: Specifies the backend server group ID. Constraints: N/A Range: N/A Default value: N/A

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.

Request Parameters

Table 5-459 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-460 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
member	Member object	Definition: Specifies the backend server.

Table 5-461 Member

Parameter	Type	Description
id	String	Definition: Specifies the backend server ID. Range: N/A NOTE The value of this parameter is not the ID of the server but an ID automatically generated for the backend server that is associated with the load balancer.
availability_zone	String	Definition: Specifies the AZ where the backend server is running. Range: N/A
name	String	Definition: Specifies the backend server name. Range: N/A Note: The name is not an ECS name.
project_id	String	Definition: Specifies the project ID of the backend server. Range: N/A
admin_state_up	Boolean	Definition: Specifies the administrative status of the backend server. Range: true or false
subnet_cidr_id	String	Definition: 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 parameter neutron_subnet_id in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets) to get the IPv4 subnet ID. You can query parameter neutron_network_id in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets) to get the IPv6 subnet ID. Range: N/A

Parameter	Type	Description
protocol_port	Integer	Definition: Specifies the port used by the backend server to receive requests. Range: N/A 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	Definition: Specifies the weight of the backend server. Requests are routed based on the load balancing algorithm configured for the backend server group and weights of backend servers. 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. Range: 0 to 100
address	String	Definition: Specifies the IP address of the backend server Range: N/A
ip_version	String	Definition: Specifies the IP address version supported by the backend server. The version depends on the value of address returned by the system. Range: v4 or v6

Parameter	Type	Description
operating_status	String	Definition: Specifies the operating status of the backend server. Range: • NO_MONITOR: No health check is configured for the backend server group to which the backend server belongs. • INITIAL: The backend server is initializing. Health check is configured for the backend server group, but no data has been reported yet. • ONLINE: The backend server is running normally. • OFFLINE: The backend server is detected unhealthy, or the cloud server used as the backend server is stopped or does not exist. • UNKNOWN: The health check has not started yet, or no listener is associated with the backend server group, or the member IP address is not assigned to a cloud service instance (such as ECS, network interface, or supplementary network interface). Multiple statuses can be used for query in the format of <i>operating_status=xxx&operating_status=xxx</i>.
status	Array of MemberStatus objects	Definition: Specifies the health status of the backend server. Range: N/A
reason	MemberHealthCheckFailedReason object	Definition: Specifies why health check fails.
created_at	String	Definition: Specifies the creation time. The value must be a UTC time in the format of <i>yyyy-MM-dd'THH:mm:ss'Z</i>. Range: N/A Note: This parameter 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	Definition: Specifies the update time. The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Range: N/A Note: This parameter 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	Definition: Specifies the backend server type. Range: • ip: IP as backend servers • instance: ECSs used as backend servers
instance_id	String	Definition: 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. Range: N/A

Table 5-462 MemberStatus

Parameter	Type	Description
listener_id	String	Definition: Specifies the listener ID. Range: N/A
operating_status	String	Definition: Specifies the operating status of the backend server. Range: • 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 ECS used as the backend server is stopped or does not exist.
reason	MemberHealthCheckFailedReason object	Definition: Specifies why the health check fails.

Parameter	Type	Description
created_at	String	Definition: Specifies the creation time. The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Range: N/A
updated_at	String	Definition: Specifies the update time. The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Range: N/A

Table 5-463 MemberHealthCheckFailedReason

Parameter	Type	Description
reason_code	String	Definition: Specifies the code of the health check failures. Range: • 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	Definition: 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 . 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. • 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	Definition: 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 . 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",
    "availability_zone" : "az1"
  },
  "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.ElClientBuilder().
        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 5-464 Path Parameters

Parameter	Mandatory	Type	Description
member_id	Yes	String	Definition: Specifies the backend server ID. Constraints: N/A Range: N/A Default value: N/A 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	Definition: Specifies the backend server group ID. Constraints: N/A Range: N/A Default value: N/A
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-465 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-466 Request body parameters

Parameter	Mandatory	Type	Description
member	Yes	UpdateMemberOption object	Definition: Request parameters for updating a backend server. Constraints: N/A

Table 5-467 UpdateMemberOption

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Definition: Specifies the administrative status of the backend server. 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 . Constraints: Please do not specify this parameter. Range: true or false Default value: N/A

Parameter	Mandatory	Type	Description
availability_zone	No	String	Definition: Specifies the AZ of the backend server. Constraints: This parameter can be only updated for IP as backend servers. If AZ affinity is enabled for the backend server group, this parameter is mandatory for IP as backend servers and cannot be changed to "". Range: AZs available for ECSs in the current region. Default value: N/A
name	No	String	Definition: Specifies the backend server name. Constraints: N/A Range: N/A Default value: N/A
weight	No	Integer	Definition: Specifies the weight of the backend server. Requests are routed based on the load balancing algorithm configured for the backend server group and weights of backend servers. 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. Constraints: This parameter is invalid when lb_algorithm is set to SOURCE_IP for the backend server group that contains the backend server. Range: 0 to 100 Default value: 1

Parameter	Mandatory	Type	Description
protocol_port	No	Integer	Definition: Specifies the port used by the backend server to receive requests. Constraints: This parameter cannot be updated if any_port_enable is set to true for a backend server group. Default value: N/A

Response Parameters

Status code: 200

Table 5-468 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
member	Member object	Definition: Response parameters for updating a backend server.

Table 5-469 Member

Parameter	Type	Description
id	String	Definition: Specifies the backend server ID. Range: N/A NOTE The value of this parameter is not the ID of the server but an ID automatically generated for the backend server that is associated with the load balancer.
availability_zone	String	Definition: Specifies the AZ where the backend server is running. Range: N/A

Parameter	Type	Description
name	String	Definition: Specifies the backend server name. Range: N/A Note: The name is not an ECS name.
project_id	String	Definition: Specifies the project ID of the backend server. Range: N/A
admin_state_up	Boolean	Definition: Specifies the administrative status of the backend server. Range: true or false
subnet_cidr_id	String	Definition: 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 parameter neutron_subnet_id in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets) to get the IPv4 subnet ID. You can query parameter neutron_network_id in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets) to get the IPv6 subnet ID. Range: N/A
protocol_port	Integer	Definition: Specifies the port used by the backend server to receive requests. Range: N/A 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	Definition: Specifies the weight of the backend server. Requests are routed based on the load balancing algorithm configured for the backend server group and weights of backend servers. 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. Range: 0 to 100
address	String	Definition: Specifies the IP address of the backend server Range: N/A
ip_version	String	Definition: Specifies the IP address version supported by the backend server. The version depends on the value of address returned by the system. Range: v4 or v6

Parameter	Type	Description
operating_status	String	Definition: Specifies the operating status of the backend server. Range: • NO_MONITOR: No health check is configured for the backend server group to which the backend server belongs. • INITIAL: The backend server is initializing. Health check is configured for the backend server group, but no data has been reported yet. • ONLINE: The backend server is running normally. • OFFLINE: The backend server is detected unhealthy, or the cloud server used as the backend server is stopped or does not exist. • UNKNOWN: The health check has not started yet, or no listener is associated with the backend server group, or the member IP address is not assigned to a cloud service instance (such as ECS, network interface, or supplementary network interface). Multiple statuses can be used for query in the format of <i>operating_status=xxx&operating_status=xxx</i> .
status	Array of MemberStatus objects	Definition: Specifies the health status of the backend server. Range: N/A
reason	MemberHealthCheckFailedReason object	Definition: Specifies why health check fails.
created_at	String	Definition: Specifies the creation time. The value must be a UTC time in the format of <i>yyyy-MM-dd'THH:mm:ss'Z'</i> . Range: N/A Note: This parameter 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	Definition: Specifies the update time. The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Range: N/A Note: This parameter 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	Definition: Specifies the backend server type. Range: • ip: IP as backend servers • instance: ECSs used as backend servers
instance_id	String	Definition: 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. Range: N/A

Table 5-470 MemberStatus

Parameter	Type	Description
listener_id	String	Definition: Specifies the listener ID. Range: N/A
operating_status	String	Definition: Specifies the operating status of the backend server. Range: • 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 ECS used as the backend server is stopped or does not exist.
reason	MemberHealthCheckFailedReason object	Definition: Specifies why the health check fails.

Parameter	Type	Description
created_at	String	Definition: Specifies the creation time. The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Range: N/A
updated_at	String	Definition: Specifies the update time. The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Range: N/A

Table 5-471 MemberHealthCheckFailedReason

Parameter	Type	Description
reason_code	String	Definition: Specifies the code of the health check failures. Range: • 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	Definition: 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 . 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. • 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	Definition: 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 . 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 huaweicloudskelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskelb.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, established persistent connections will be maintained.

Calling Method

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

URI

DELETE /v3/{project_id}/elb/pools/{pool_id}/members/{member_id}

Table 5-472 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Parameter	Mandatory	Type	Description
pool_id	Yes	String	Definition: Specifies the backend server group ID. Constraints: N/A Range: N/A Default value: N/A
member_id	Yes	String	Definition: Specifies the backend server ID. The member ID can be obtained by querying the backend server list . Constraints: N/A Range: N/A Default value: N/A 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 5-473 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 204

Successful request.

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 huaweicloudskelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskelb.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 in a Project

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 5-474 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Table 5-475 Query Parameters

Parameter	Mandatory	Type	Description
marker	No	String	Definition: Specifies the ID of the last record on the previous page. Constraints: • This parameter must be used together with limit. • If the parameter is not specified, only resources on the first page are queried. • This parameter cannot be left blank or set to an invalid ID. Range: N/A Default value: N/A
limit	No	Integer	Definition: Specifies the number of records returned on each page. Constraints: N/A Range: 0 to 2000 Default value: 2000

Parameter	Mandatory	Type	Description
page_reverse	No	Boolean	Definition: Specifies whether to use reverse query. Constraints: • This parameter must be used together with limit. • If page_reverse is set to true and you want to query the resources on the previous page, set the value of marker to the value of previous_marker. Range: • true: Query resources on the previous page. • false: Query resources on the next page. Default value: false
name	No	Array of strings	Definition: Specifies the backend server name. Multiple names can be used for query in the format of <i>name=xxx&name=xxx</i>. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
weight	No	Array of integers	Definition: 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 set to 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 used for query in the format of <i>weight=xxx&weight=xxx</i>. Constraints: N/A Range: N/A Default value: N/A
admin_state_up	No	Boolean	Definition: Specifies the administrative status of the backend server. 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. Constraints: N/A Range: true or false Default value: N/A

Parameter	Mandatory	Type	Description
subnet_cidr_id	No	Array of strings	Definition: 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 associated with the backend server. Only IPv4 subnets are supported. Multiple IDs can be used for query in the format of <i>subnet_cidr_id=xxx&subnet_cidr_id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
address	No	Array of strings	Definition: 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. Multiple IP addresses can be used for query in the format of <i>address=xxx&address=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
protocol_port	No	Array of integers	Definition: Specifies the port used by the backend servers. Multiple ports can be used for query in the format of <i>protocol_port=xxx&protocol_port=xxx</i> . Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
id	No	Array of strings	Definition: Specifies the backend server ID. Multiple IDs can be used for query in the format of <i>id=xxx&id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
operating_status	No	Array of strings	Definition: Specifies the operating status of the backend server. Multiple statuses can be used for query in the format of <i>operating_status=xxx&operating_status=xxx</i>. Constraints: N/A Range: • NO_MONITOR: No health check is configured for the backend server group to which the backend server belongs. • INITIAL: The backend server is initializing. Health check is configured for the backend server group, but no data has been reported yet. • ONLINE: The backend server is running normally. • OFFLINE: The backend server is detected unhealthy, or the cloud server used as the backend server is stopped or does not exist. • UNKNOWN: The health check has not started yet, or no listener is associated with the backend server group, or the member IP address is not assigned to a cloud service instance (such as ECS, network interface, or supplementary network interface). Default value: N/A

Parameter	Mandatory	Type	Description
enterprise_project_id	No	Array of strings	Definition: Specifies the ID of the enterprise project. Multiple values can be used for query in the format of <i>enterprise_project_id=xxx&enterprise_project_id=xxx</i>. Constraints: • 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. Range: N/A Default value: N/A
ip_version	No	Array of strings	Definition: Specifies the IP address version. Multiple versions can be used for query in the format of <i>ip_version=xxx&ip_version=xxx</i>. Constraints: N/A Range: v4 or v6 Default value: N/A

Parameter	Mandatory	Type	Description
pool_id	No	Array of strings	Definition: Specifies the ID of the backend server group to which the backend server belongs. Multiple IDs can be used for query in the format of <i>pool_id=xxx&pool_id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
loadbalancer_id	No	Array of strings	Definition: Specifies the ID of the load balancer. Multiple IDs can be used for query in the format of <i>loadbalancer_id=xxx&loadbalancer_id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-476 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-477 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
page_info	PageInfo object	Definition: Specifies the pagination information.
members	Array of MemberInfo objects	Definition: Specifies the backend servers.

Table 5-478 PageInfo

Parameter	Type	Description
previous_marker	String	Definition: Specifies the ID of the first record in the pagination query result. If page_reverse is set to true , this parameter is used together to query resources on the previous page. Range: N/A
next_marker	String	Definition: Specifies the ID of the last record in the pagination query result. It is usually used to query resources on the next page. Range: N/A
current_count	Integer	Definition: Specifies the number of records returned on the current page. Range: N/A

Table 5-479 MemberInfo

Parameter	Type	Description
id	String	Definition: Specifies the backend server ID. Range: N/A NOTE The value of this parameter is not the ID of the server but an ID automatically generated for the backend server that is associated with the load balancer.

Parameter	Type	Description
availability_zone	String	Specifies the AZ where the backend server is running. Range: N/A
name	String	Definition: Specifies the backend server name. Range: N/A Note: The name is not an ECS name.
project_id	String	Specifies the ID of the project where the backend server is used. Range: N/A
pool_id	String	Definition: Specifies the ID of the backend server group to which the backend server belongs. Range: N/A This parameter is unsupported. Please do not use it.
admin_state_up	Boolean	Definition: Specifies the administrative status of the backend server. 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 . Range: true or false
subnet_cidr_id	String	Definition: 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 parameter neutron_subnet_id in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets) to get the IPv4 subnet ID. You can query parameter neutron_network_id in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets) to get the IPv6 subnet ID. Range: N/A

Parameter	Type	Description
protocol_port	Integer	Definition: Specifies the port used by the backend server to receive requests. Range: N/A
weight	Integer	Definition: Specifies the weight of the backend server. Requests are routed based on the load balancing algorithm configured for the backend server group and weights of backend servers. 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. Range: 0 to 100
address	String	Definition: Specifies the IP address bound to the backend server. Range: • If subnet_cidr_id is left blank, IP as backend servers will be added. In this case, the IP address must be an IPv4 address. • If subnet_cidr_id is not left blank, ECSs, BMSs, or supplementary network interfaces will be added as backend servers. It must be in the subnet specified by subnet_cidr_id.
ip_version	String	Definition: Specifies the IP address version supported by the backend server. The version depends on the value of address returned by the system. Range: v4 or v6

Parameter	Type	Description
device_owner	String	Definition: Specifies whether the backend server is associated with an ECS. Range: • 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	Definition: 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. Range: N/A This parameter is unsupported. Please do not use it.

Parameter	Type	Description
operating_status	String	Definition: Specifies the operating status of the backend server if listener_id under status is not specified. Range: • NO_MONITOR: No health check is configured for the backend server group to which the backend server belongs. • INITIAL: The backend server is initializing. Health check is configured for the backend server group, but no data has been reported yet. • ONLINE: The backend server is running normally. • OFFLINE: The backend server is detected unhealthy, or the cloud server used as the backend server is stopped or does not exist. • UNKNOWN: The health check has not started yet, or no listener is associated with the backend server group, or the member IP address is not assigned to a cloud service instance (such as ECS, network interface, or supplementary network interface).
status	Array of MemberStatus objects	Definition: 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	Definition: Specifies the ID of the load balancer. This parameter is unsupported. Please do not use it.
loadbalancers	Array of ResourceID objects	Definition: Specifies the IDs of the load balancers associated with the backend server. This parameter is unsupported. Please do not use it.

Parameter	Type	Description
created_at	String	Definition: Specifies the creation time. The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Range: N/A Note: This parameter 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	Definition: Specifies the update time. The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Range: N/A Note: This parameter 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	Definition: Specifies the type of the backend server. Range: • ip: IP as backend servers • instance: ECSs used as backend servers
instance_id	String	Definition: 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. Range: N/A
reason	MemberHealthCheckFailedReason object	Definition: Specifies why health check fails.

Table 5-480 MemberStatus

Parameter	Type	Description
listener_id	String	Definition: Specifies the listener ID. Range: N/A

Parameter	Type	Description
operating_status	String	Definition: Specifies the operating status of the backend server. Range: • 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 ECS used as the backend server is stopped or does not exist.
reason	MemberHealthCheckFailedReason object	Definition: Specifies why the health check fails.
created_at	String	Definition: Specifies the creation time. The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Range: N/A
updated_at	String	Definition: Specifies the update time. The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Range: N/A

Table 5-481 ResourceID

Parameter	Type	Description
id	String	Definition: Specifies the resource ID.

Table 5-482 MemberHealthCheckFailedReason

Parameter	Type	Description
reason_code	String	Definition: Specifies the code of the health check failures. Range: • 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	Definition: 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 . 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. • 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	Definition: 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 . 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:az1",
    "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:az1",
    "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.getStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from 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.ElbcClientBuilder().
            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 5-483 Path Parameters

Parameter	Mandatory	Type	Description
pool_id	Yes	String	Definition: Specifies the backend server group ID. Constraints: N/A Range: N/A Default value: N/A
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-484 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-485 Request body parameters

Parameter	Mandatory	Type	Description
members	Yes	Array of BatchCreateMembersOption objects	Definition: Specifies the request parameters for adding backend servers in batches. Constraints: N/A

Table 5-486 BatchCreateMembersOption

Parameter	Mandatory	Type	Description
name	No	String	Definition: Specifies the backend server name. Constraints: N/A Range: N/A Default value: N/A
availability_zone	No	String	Definition: Specifies the AZ of the backend server. Constraints: This parameter can be only set for IP as backend servers. If AZ affinity is enabled for the backend server group, this parameter must be set to a valid value for IP as backend servers. Range: AZs available for ECSs in the current region. Default value: N/A

Parameter	Mandatory	Type	Description
address	Yes	String	Definition: 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. Constraints: If subnet_cidr_id is left blank, IP as backend servers will be added. In this case, the IP address must be an IPv4 address. Range: N/A Default value: N/A
protocol_port	Yes	Integer	Definition: Specifies the port used by the backend server to receive requests. Constraints: N/A Range: N/A Default value: N/A 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	Definition: 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 parameter neutron_subnet_id in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets) to get the IPv4 subnet ID. You can query parameter neutron_network_id in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets) to get the IPv6 subnet ID. Constraints: • 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, indicating that an IP as backend server will be added. 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. Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
weight	No	Integer	Definition: Specifies the weight of the backend server. Requests are routed based on the load balancing algorithm configured for the backend server group and weights of backend servers. 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. Constraints: This parameter is invalid when lb_algorithm is set to SOURCE_IP for the backend server group that contains the backend server. Range: 0 to 100 Default value: 1

Response Parameters

Status code: 201

Table 5-487 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
members	Array of BatchMember objects	Definition: Specifies the backend servers.

Table 5-488 BatchMember

Parameter	Type	Description
id	String	Definition: Specifies the backend server ID. Range: N/A NOTE The value of this parameter is not the ID of the server but an ID automatically generated for the backend server that is associated with the load balancer.
name	String	Definition: Specifies the backend server name. Range: N/A
project_id	String	Specifies the ID of the project where the backend server is used. Range: N/A
admin_state_up	Boolean	Definition: Specifies the administrative status of the backend server. Range: true or false
subnet_cidr_id	String	Definition: 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 parameter neutron_subnet_id in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets) to get the IPv4 subnet ID. You can query parameter neutron_network_id in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets) to get the IPv6 subnet ID. Range: N/A
protocol_port	Integer	Definition: Specifies the port used by the backend server to receive requests. Range: N/A 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	Definition: Specifies the weight of the backend server. Requests are routed based on the load balancing algorithm configured for the backend server group and weights of backend servers. 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. Range: 0 to 100 Default value: N/A
address	String	Definition: Specifies the IP address of the backend server Range: N/A
operating_status	String	Definition: Specifies the operating status of the backend server. Range: • NO_MONITOR: No health check is configured for the backend server group to which the backend server belongs. • INITIAL: The backend server is initializing. Health check is configured for the backend server group, but no data has been reported yet. • ONLINE: The backend server is running normally. • OFFLINE: The backend server is detected unhealthy, or the cloud server used as the backend server is stopped or does not exist. • UNKNOWN: The health check has not started yet, or no listener is associated with the backend server group, or the member IP address is not assigned to a cloud service instance (such as ECS, network interface, or supplementary network interface).
reason	MemberHealthCheckFailedReason object	Definition: Specifies why the health check fails.

Parameter	Type	Description
status	Array of MemberStatus objects	Definition: 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	Definition: Specifies the type of the backend server. Range: • ip: IP as backend servers • instance: ECSs used as backend servers
instance_id	String	Definition: 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. Range: N/A
port_id	String	Definition: Specifies the ID of the VPC port bound to the IP address. Range: N/A
ret_status	String	Definition: Specifies the status of adding a backend server. Range: • successful: The backend server is added. • existed: The backend server already exists.
created_at	String	Definition: Specifies the creation time. The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Range: N/A Note: This parameter 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	Definition: Specifies the update time. The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Range: N/A Note: This parameter 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 MemberStatus

Parameter	Type	Description
listener_id	String	Definition: Specifies the listener ID. Range: N/A
operating_status	String	Definition: Specifies the operating status of the backend server. Range: • 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 ECS used as the backend server is stopped or does not exist.
reason	MemberHealthCheckFailedReason object	Definition: Specifies why the health check fails.
created_at	String	Definition: Specifies the creation time. The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Range: N/A
updated_at	String	Definition: Specifies the update time. The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Range: N/A

Table 5-490 MemberHealthCheckFailedReason

Parameter	Type	Description
reason_code	String	Definition: Specifies the code of the health check failures. Range: • 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	Definition: 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 . 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. • 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	Definition: 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 . 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

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",
    "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.getErrMsg());
        }
    }
}
```

```
}  
}
```

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	Successful request.

Error Codes

See [Error Codes](#).

5.12.8 Batch Removing Backend Servers

Function

This API is used to remove 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 5-491 Path Parameters

Parameter	Mandatory	Type	Description
pool_id	Yes	String	Definition: Specifies the backend server group ID. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-492 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-493 Request body parameters

Parameter	Mandatory	Type	Description
members	Yes	Array of BatchDeleteMembersOption objects	Definition: Specifies the request body for removing backend servers in batches. Constraints: N/A

Table 5-494 BatchDeleteMembersOption

Parameter	Mandatory	Type	Description
id	No	String	Definition: Specifies the ID of the backend server to be deleted. Constraints: If id is passed, other parameters cannot be specified. Otherwise, an error will be reported. Range: N/A Default value: N/A 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.
address	No	String	Definition: Specifies the IP address bound to the backend server. Constraints: • address and protocol_port must be passed at the same time. • id cannot be passed together with address and protocol_port. Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
protocol_port	No	Integer	Definition: Specifies the port used by the backend server to receive requests. Constraints: • 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 with any_port_enable set to true. Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-495 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
members	Array of BatchDeleteMembersState objects	Definition: Specifies the backend servers.

Table 5-496 BatchDeleteMembersState

Parameter	Type	Description
id	String	Definition: Specifies the backend server ID. Range: N/A NOTE The value of this parameter is not the ID of the server but an ID automatically generated for the backend server that is associated with the load balancer.
ret_status	String	Definition: Specifies the status of deleting the backend server. Range: • successful: The backend server is deleted. • not found: The backend server does not exist.

Example Requests

- Removing 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"
  } ]
}
```

- Removing 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

Successful request.

```
{
  "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

- Removing 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());
    }
}
```

- Removing 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

- Removing 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)
```

- Removing 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

- Removing 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.ElClientBuilder().
        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)
}
}
```

- Removing 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.ElClientBuilder().
            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	Successful request.

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 5-497 Path Parameters

Parameter	Mandatory	Type	Description
pool_id	Yes	String	Definition: Specifies the backend server group ID. Constraints: N/A Range: N/A Default value: N/A
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-498 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-499 Request body parameters

Parameter	Mandatory	Type	Description
members	Yes	Array of BatchUpdateMembersOption objects	Definition: Specifies the backend server. Range: N/A

Table 5-500 BatchUpdateMembersOption

Parameter	Mandatory	Type	Description
id	Yes	String	Definition: Specifies the backend server ID. Constraints: N/A Range: N/A Default value: N/A 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.
availability_zone	No	String	Definition: Specifies the AZ of the backend server. Constraints: This parameter can be only set for IP as backend servers. If AZ affinity is enabled for the backend server group, this parameter must be set to a valid value for IP as backend servers. Range: AZs available for ECSs in the current region. Default value: N/A
admin_state_up	No	Boolean	Specifies the administrative status of the backend server. Constraints: 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 . Range: N/A Default value: N/A Please do not specify this parameter.
name	No	String	Definition: Specifies the backend server name. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
protocol_port	No	Integer	Definition: Specifies the port used by the backend server to receive requests. Constraints: This parameter cannot be updated if any_port_enable is set to true for a backend server group. Range: 1-65535 Default value: N/A
weight	No	Integer	Definition: Specifies the weight of the backend server. Requests are routed based on the load balancing algorithm configured for the backend server group and weights of backend servers. If the weight is set to 0, the backend server will not accept new requests. Constraints: This parameter is invalid when lb_algorithm is set to SOURCE_IP for the backend server group that contains the backend server. Range: 0 to 100 Default value: N/A

Response Parameters

Status code: 200

Table 5-501 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
members	Array of BatchUpdateMember objects	Definition: Specifies the backend servers.

Table 5-502 BatchUpdateMember

Parameter	Type	Description
id	String	Definition: Specifies the backend server ID. Range: N/A NOTE The value of this parameter is not the ID of the server but an ID automatically generated for the backend server that is associated with the load balancer.
name	String	Definition: Specifies the backend server name. Range: N/A
project_id	String	Specifies the ID of the project where the backend server is used. Range: N/A
admin_state_up	Boolean	Specifies the administrative status of the backend server. 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 . Range: N/A
subnet_cidr_id	String	Definition: 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 parameter neutron_subnet_id in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets) to get the IPv4 subnet ID. You can query parameter neutron_network_id in the response by calling the API (GET https://{VPC_Endpoint}/v1/{project_id}/subnets) to get the IPv6 subnet ID. Range: N/A

Parameter	Type	Description
protocol_port	Integer	Definition: Specifies the port used by the backend server to receive requests. Range: N/A 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	Definition: Specifies the weight of the backend server. Requests are routed based on the load balancing algorithm configured for the backend server group and weights of backend servers. 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. Range: 0 to 100
address	String	Definition: Specifies the IP address of the backend server Range: N/A

Parameter	Type	Description
operating_status	String	Definition: Specifies the operating status of the backend server. Range: • NO_MONITOR: No health check is configured for the backend server group to which the backend server belongs. • INITIAL: The backend server is initializing. Health check is configured for the backend server group, but no data has been reported yet. • ONLINE: The backend server is running normally. • OFFLINE: The backend server is detected unhealthy, or the cloud server used as the backend server is stopped or does not exist. • UNKNOWN: The health check has not started yet, or no listener is associated with the backend server group, or the member IP address is not assigned to a cloud service instance (such as ECS, network interface, or supplementary network interface).
reason	MemberHealthCheckFailedReason object	Definition: Specifies why health check fails.
status	Array of MemberStatus objects	Definition: 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	Definition: Specifies the type of the backend server. Range: • ip: IP as backend servers • instance: ECSs used as backend servers

Parameter	Type	Description
instance_id	String	Definition: 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. Range: N/A
port_id	String	Definition: Specifies the ID of the VPC port bound to the IP address. Range: N/A
created_at	String	Definition: Specifies the creation time. The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Range: N/A Note: This parameter 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	Definition: Specifies the update time. The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Range: N/A Note: This parameter will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.
availability_zone	String	Specifies the AZ where the backend server is running. Range: N/A

Table 5-503 MemberStatus

Parameter	Type	Description
listener_id	String	Definition: Specifies the listener ID. Range: N/A

Parameter	Type	Description
operating_status	String	Definition: Specifies the operating status of the backend server. Range: • 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 ECS used as the backend server is stopped or does not exist.
reason	MemberHealthCheckFailedReason object	Definition: Specifies why the health check fails.
created_at	String	Definition: Specifies the creation time. The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Range: N/A
updated_at	String	Definition: Specifies the update time. The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Range: N/A

Table 5-504 MemberHealthCheckFailedReason

Parameter	Type	Description
reason_code	String	Definition: Specifies the code of the health check failures. Range: • 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	Definition: 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 . 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. • 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	Definition: 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 . 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](#).

5.12.10 Creating a Backend Server Check Task

Function

This API is used to create a task for checking the configurations, network ACL rules, and security group rules of a backend server.

Calling Method

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

URI

POST /v3/{project_id}/elb/members/{member_id}/health-check

Table 5-505 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
member_id	Yes	String	Definition: Specifies the backend server ID. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-506 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-507 Request body parameters

Parameter	Mandatory	Type	Description
member_check	No	CreateMemberHealthCheckJobOption object	Definition: Specifies the request parameters for creating a backend server check task.

Table 5-508 CreateMemberHealthCheckJobOption

Parameter	Mandatory	Type	Description
listener_id	Yes	String	Definition: Specifies the ID of a listener to query the status of the backend servers that are associated with this listener. Range: N/A
subject	Yes	String	Definition: Specifies the check items. Range: • securityGroup: security group checks • networkAcl: network ACL checks • config: health check port checks • all: all check items

Response Parameters

Status code: 201

Table 5-509 Response body parameters

Parameter	Type	Description
member_check	MemberCheckJob object	Definition: Specifies the information about the backend server check task.
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

Table 5-510 MemberCheckJob

Parameter	Type	Description
job_id	String	Definition: Specifies the task ID that is used to query the task execution result. Range: N/A

Example Requests

Creating a backend server check task

```
POST https://{ELB_Endpoint}/v3/0c1503d710984bad92306faea3654dfd/elb/members/  
02272819-5655-4c6b-892b-105604f6aea0/health-check
```

```
{  
  "member_check": {  
    "listener_id": "b445cc43-02d7-4863-9481-283b7fb1c222",  
    "subject": "all"  
  }  
}
```

Example Responses

Status code: 201

Successful request.

```
{  
  "member_check": {  
    "job_id": "919221ce-0011-4558-81ca-2866e6e68a27"  
  },  
  "request_id": "9869f52f-b740-4075-bb29-6dd0008a1f1d"  
}
```

SDK Sample Code

The SDK sample code is as follows.

Java

Creating a backend server check task

```
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 CreateMemberHealthCheckJobSolution {

    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();

        CreateMemberHealthCheckJobRequest request = new CreateMemberHealthCheckJobRequest();
        request.withMemberId("{member_id}");
        CreateMemberHealthCheckJobRequestBody body = new CreateMemberHealthCheckJobRequestBody();
        CreateMemberHealthCheckJobOption memberCheckbody = new
        CreateMemberHealthCheckJobOption();
        memberCheckbody.withListenerId("b445cc43-02d7-4863-9481-283b7fb1c222")
            .withSubject("all");
        body.withMemberCheck(memberCheckbody);
        request.withBody(body);
        try {
            CreateMemberHealthCheckJobResponse response = client.createMemberHealthCheckJob(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 check task

```
# 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 = CreateMemberHealthCheckJobRequest()
        request.member_id = "{member_id}"
        memberCheckbody = CreateMemberHealthCheckJobOption(
            listener_id="b445cc43-02d7-4863-9481-283b7fb1c222",
            subject="all"
        )
        request.body = CreateMemberHealthCheckJobRequestBody(
            member_check=memberCheckbody
        )
        response = client.create_member_health_check_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

Creating a backend server check task

```
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.CreateMemberHealthCheckJobRequest{}
request.MemberId = "{member_id}"
memberCheckbody := &model.CreateMemberHealthCheckJobOption{
    ListenerId: "b445cc43-02d7-4863-9481-283b7fb1c222",
    Subject: "all",
}
request.Body = &model.CreateMemberHealthCheckJobRequestBody{
    MemberCheck: memberCheckbody,
}
response, err := client.CreateMemberHealthCheckJob(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	Successful request.

Error Codes

See [Error Codes](#).

5.12.11 Querying the Results of a Backend Server Check Task

Function

This API is used to query the results of a backend server check task.

Calling Method

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

URI

GET /v3/{project_id}/elb/members/check/jobs/{job_id}

Table 5-511 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
job_id	Yes	String	Definition: Specifies the task ID returned by the API for creating a backend server check task.

Request Parameters

Table 5-512 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-513 Response body parameters

Parameter	Type	Description
member_check	MemberCheckJobInfo object	Definition: Specifies the information about the backend server check task.
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

Table 5-514 MemberCheckJobInfo

Parameter	Type	Description
status	String	Definition: Specifies the result of a backend server check task. The value can be processed , processing , or failed . Range: N/A
result	MemberCheckJobResult object	Definition: Specifies the result of each check item.
created_at	String	Definition: Specifies the task creation time. Range: N/A
updated_at	String	Definition: Specifies the task update time. Range: N/A
job_id	String	Definition: Specifies the task ID.
check_item_total_num	Integer	Definition: Specifies the total number of check items. Range: N/A
check_item_finished_num	Integer	Definition: Specifies the number of checked items. Range: N/A
listener_id	String	Definition: Specifies the ID of a listener to query the status of the backend servers that are associated with this listener. Range: N/A
member_id	String	Definition: Specifies the backend server ID. Range: N/A

Table 5-515 MemberCheckJobResult

Parameter	Type	Description
config	MemberCheckJobResultGroup object	Definition: Specifies the configuration check. Range: N/A

Parameter	Type	Description
acl	MemberCheckJobResultGroup object	Definition: Specifies the network ACL rule check. Range: N/A
security_group	MemberCheckJobResultGroup object	Definition: Specifies the security group rule check. Range: N/A

Table 5-516 MemberCheckJobResultGroup

Parameter	Type	Description
check_result	Boolean	Definition: Specifies the check result. true indicates that the check is passed, and false indicates that the check is not passed. Range: N/A
check_items	Array of MemberCheckJobResultItem objects	Definition: Specifies the summary of grouped check items.
check_status	String	Definition: Specifies the result of a backend server check task. The value can be processed , processing , or failed . Range: N/A

Table 5-517 MemberCheckJobResultItem

Parameter	Type	Description
name	String	Definition: Specifies the check item name. Range: N/A
reason	String	Definition: Specifies the exception cause. Range: N/A
severity	String	Definition: Specifies the exception severity, which can be Major (severe) or Tips (informational). Range: N/A

Parameter	Type	Description
subject	String	Definition: Specifies the check type. config indicates configuration check. Range: N/A
job_id	String	Definition: Specifies the task ID. Range: N/A
reason_template	String	Definition: Specifies the exception reason template. Range: N/A
reason_params	Array of strings	Definition: Specifies the exception variables, which is used to dynamically generate exception causes based on the exception cause template. Range: N/A

Example Requests

Querying the results of a backend server check task

```
POST https://{ELB_Endpoint}/v3/04dd36f964000fe22f9ac00bc85b1a1d/elb/members/check/jobs/04a9bc65-b75b-478d-b4d6-e693bb61dd35
```

Example Responses

Status code: 200

Successful request.

```
{
  "member_check" : {
    "status" : "processed",
    "result" : {
      "config" : {
        "check_result" : true,
        "check_items" : [ {
          "name" : "check_hc_config_port",
          "reason" : null,
          "severity" : "Tips",
          "subject" : "config",
          "job_id" : "919221ce-0011-4558-81ca-2866e6e68a27",
          "reason_template" : "healthCheck {$hm_id}'s protocolPort {$protocol_port} is different from member port {$member_port}",
          "reason_params" : [ ]
        } ],
        "check_status" : "processed"
      },
      "acl" : {
        "check_result" : true,
        "check_items" : [ {
          "name" : "acl_check_hc_protocol_egress",
          "reason" : null,
          "severity" : "Major",
          "subject" : "networkAcl",
          "job_id" : "919221ce-0011-4558-81ca-2866e6e68a27",
          "reason_template" : "healthCheck {$hm_id}'s protocol is {$hc_protocol}, but the transport layer
```

```
protocol corresponding to the protocol {$trans_protocol} is not allowed by ACL {$acl_id} egress policies",
  "reason_params" : [ ]
}, {
  "name" : "acl_check_hc_dest_port_egress",
  "reason" : null,
  "severity" : "Major",
  "subject" : "networkAcl",
  "job_id" : "919221ce-0011-4558-81ca-2866e6e68a27",
  "reason_template" : "healthCheck destination port may not allowed by ACL {$acl_id} egress policies,
it is recommended to open all destination ports",
  "reason_params" : [ ]
}, {
  "name" : "acl_check_hc_dest_ip_egress",
  "reason" : null,
  "severity" : "Major",
  "subject" : "networkAcl",
  "job_id" : "919221ce-0011-4558-81ca-2866e6e68a27",
  "reason_template" : "healthCheck destination IP {$dest_ip} is not allowed by ACL {$acl_id} egress
policies",
  "reason_params" : [ ]
}, {
  "name" : "acl_check_hc_source_port_egress",
  "reason" : null,
  "severity" : "Major",
  "subject" : "networkAcl",
  "job_id" : "919221ce-0011-4558-81ca-2866e6e68a27",
  "reason_template" : "healthCheck source port {$source_port} is not allowed by ACL {$acl_id} egress
policies",
  "reason_params" : [ ]
}, {
  "name" : "acl_check_hc_source_ip_egress",
  "reason" : null,
  "severity" : "Major",
  "subject" : "networkAcl",
  "job_id" : "919221ce-0011-4558-81ca-2866e6e68a27",
  "reason_template" : "healthCheck source IP {$source_ip} is not allowed by ACL {$acl_id} egress
policies",
  "reason_params" : [ ]
}, {
  "name" : "acl_check_hc_protocol_ingress",
  "reason" : null,
  "severity" : "Major",
  "subject" : "networkAcl",
  "job_id" : "919221ce-0011-4558-81ca-2866e6e68a27",
  "reason_template" : "healthCheck {$hm_id}'s protocol is {$hc_protocol}, but the transport layer
protocol corresponding to the protocol {$trans_protocol} is not allowed by ACL {$acl_id} ingress policies",
  "reason_params" : [ ]
}, {
  "name" : "acl_check_hc_dest_port_ingress",
  "reason" : null,
  "severity" : "Major",
  "subject" : "networkAcl",
  "job_id" : "919221ce-0011-4558-81ca-2866e6e68a27",
  "reason_template" : "healthCheck destination port {$dest_port} is not allowed by ACL {$acl_id}
ingress policies",
  "reason_params" : [ ]
}, {
  "name" : "acl_check_hc_dest_ip_ingress",
  "reason" : null,
  "severity" : "Major",
  "subject" : "networkAcl",
  "job_id" : "919221ce-0011-4558-81ca-2866e6e68a27",
  "reason_template" : "healthCheck destination IP {$dest_ip} is not allowed by ACL {$acl_id} ingress
policies",
  "reason_params" : [ ]
}, {
  "name" : "acl_check_hc_source_port_ingress",
  "reason" : null,
  "severity" : "Tips",
```

```
"subject" : "networkAcl",
"job_id" : "919221ce-0011-4558-81ca-2866e6e68a27",
"reason_template" : "healthCheck source port may not allowed by ACL {$acl_id} ingress policies, it is recommended to open all destination ports",
"reason_params" : [ ]
}, {
  "name" : "acl_check_hc_source_ip_ingress",
  "reason" : null,
  "severity" : "Major",
  "subject" : "networkAcl",
  "job_id" : "919221ce-0011-4558-81ca-2866e6e68a27",
  "reason_template" : "healthCheck source IP {$source_ip} is not allowed by ACL {$acl_id} ingress policies",
  "reason_params" : [ ]
}],
"check_status" : "processed"
},
"security_group" : {
  "check_result" : true,
  "check_items" : [ {
    "name" : "security_group_check_hc_protocol_egress",
    "reason" : null,
    "severity" : "Major",
    "subject" : "securityGroup",
    "job_id" : "919221ce-0011-4558-81ca-2866e6e68a27",
    "reason_template" : "healthCheck {$hm_id}'s protocol is {$hc_protocol}, but the transport layer protocol corresponding to the protocol {$transport_protocol} is not allowed by securityGroup {$security_group_id} egress rules",
    "reason_params" : [ ]
  }, {
    "name" : "security_group_check_hc_port_egress",
    "reason" : null,
    "severity" : "Major",
    "subject" : "securityGroup",
    "job_id" : "919221ce-0011-4558-81ca-2866e6e68a27",
    "reason_template" : "healthCheck dest port {$dest_port} is not allowed by securityGroup {$security_group_id} egress rules",
    "reason_params" : [ ]
  }, {
    "name" : "security_group_check_hc_source_ip_egress",
    "reason" : null,
    "severity" : "Major",
    "subject" : "securityGroup",
    "job_id" : "919221ce-0011-4558-81ca-2866e6e68a27",
    "reason_template" : "healthCheck source IP {$source_ip} is not allowed by securityGroup {$security_group_id} egress rules",
    "reason_params" : [ ]
  }, {
    "name" : "security_group_check_hc_protocol_ingress",
    "reason" : null,
    "severity" : "Major",
    "subject" : "securityGroup",
    "job_id" : "919221ce-0011-4558-81ca-2866e6e68a27",
    "reason_template" : "healthCheck {$hm_id}'s protocol is {$hc_protocol}, but the transport layer protocol corresponding to the protocol {$transport_protocol} is not allowed by securityGroup {$security_group_id} ingress rules",
    "reason_params" : [ ]
  }, {
    "name" : "security_group_check_hc_port_ingress",
    "reason" : null,
    "severity" : "Major",
    "subject" : "securityGroup",
    "job_id" : "919221ce-0011-4558-81ca-2866e6e68a27",
    "reason_template" : "healthCheck dest port {$dest_port} is not allowed by securityGroup {$security_group_id} ingress rules",
    "reason_params" : [ ]
  }, {
    "name" : "security_group_check_hc_source_ip_ingress",
    "reason" : null,
```

```
        "severity" : "Major",
        "subject" : "securityGroup",
        "job_id" : "919221ce-0011-4558-81ca-2866e6e68a27",
        "reason_template" : "healthCheck source IP {$source_ip} is not allowed by securityGroup
{$security_group_id} ingress rules",
        "reason_params" : [ ]
    } ],
    "check_status" : "processed"
}
},
"created_at" : "2024-12-08T07:55:04Z",
"updated_at" : "2024-12-08T07:55:05Z",
"job_id" : "919221ce-0011-4558-81ca-2866e6e68a27",
"check_item_total_num" : 17,
"check_item_finished_num" : 17,
"listener_id" : "b445cc43-02d7-4863-9481-283b7fb1c222",
"member_id" : "02272819-5655-4c6b-892b-105604f6aea0"
},
"request_id" : "5980e624-dc64-46b9-8d74-e5834655dab5"
}
```

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 ShowMemberHealthCheckJobSolution {

    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();
        ShowMemberHealthCheckJobRequest request = new ShowMemberHealthCheckJobRequest();
        request.withJobId("{job_id}");
        try {
            ShowMemberHealthCheckJobResponse response = client.showMemberHealthCheckJob(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        }
    }
}
```

```
        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 huaweicloudskgelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskgelb.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 = ShowMemberHealthCheckJobRequest()
        request.job_id = "{job_id}"
        response = client.show_member_health_check_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.ShowMemberHealthCheckJobRequest{}
request.JobId = "{job_id}"
response, err := client.ShowMemberHealthCheckJob(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

This API has the following 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 5-518 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-519 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-520 Request body parameters

Parameter	Mandatory	Type	Description
healthmonitor	Yes	CreateHealthMonitorOption object	Definition: Specifies the request parameters for configuring a health check. Constraints: N/A

Table 5-521 CreateHealthMonitorOption

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Definition: Specifies the administrative status of the health check. Constraints: N/A Range: • true: The health check function is enabled. • false: The health check function is disabled. Default value: true
delay	Yes	Integer	Definition: Specifies the interval between health checks, in seconds. Constraints: N/A Range: 1 to 50 Default value: N/A
domain_name	No	String	Definition: Specifies the domain name that HTTP requests are sent to during the health check. Constraints: This parameter is available only when type is set to HTTP or HTTPS . Range: The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter. Default value: 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.

Parameter	Mandatory	Type	Description
expected_codes	No	String	Definition: Specifies the expected HTTP status code. Constraints: This parameter will take effect only when type is set to HTTP , HTTPS or GRPC . Range: • 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 Default value: If type is set to GRPC , the default value is 0 . If type is set to other protocols, the default value is 200 .
http_method	No	String	Definition: Specifies the HTTP method. Constraints: This parameter is available when type is set to HTTP or HTTPS . Range: GET , HEAD , or POST Default value: GET
max_retries	Yes	Integer	Definition: Specifies the number of consecutive health checks when the health check result of a backend server changes from OFFLINE to ONLINE . Constraints: N/A Range: 1 to 10 Default value: N/A
max_retries_down	No	Integer	Definition: Specifies the number of consecutive health checks when the health check result of a backend server changes from ONLINE to OFFLINE . Constraints: N/A Range: 1 to 10 Default value: N/A

Parameter	Mandatory	Type	Description
monitor_port	No	Integer	Definition: Specifies the health check port. Constraints: This parameter is required if any_port_enable is set to true for the backend server group. Range: 1 to 65535, or null (the port of a backend server will be used by default). Default value: null
name	No	String	Definition: Specifies the health check name. Constraints: N/A Range: N/A Default value: N/A
pool_id	Yes	String	Definition: Specifies the ID of the backend server group for which the health check is configured. Constraints: N/A Range: N/A Default value: N/A
project_id	No	String	Specifies the project ID of the health check. Constraints: N/A Range: N/A Default value: N/A
timeout	Yes	Integer	Definition: 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 . Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
type	Yes	String	Definition: Specifies the health check protocol. Constraints: • 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. Range: The value can be TCP, UDP_CONNECT, HTTP, HTTPS, GRPC, or TLS. Default value: N/A

Parameter	Mandatory	Type	Description
url_path	No	String	Definition: Specifies the HTTP request path for the health check. The value must start with a slash (/), and the default value is /. Constraints: This parameter is available only when type is set to HTTP or HTTPS . Range: The value can contain letters, digits, hyphens (-), slashes (/), periods (.), percentage signs (%), question marks (?), pound signs (#), ampersand signs (&), and the extended character set: _~!()*[]@\$^:'+,. Default value: N/A

Response Parameters

Status code: 201

Table 5-522 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
healthmonitor	HealthMonitor object	Definition: Specifies the response parameters for configuring a health check. Constraints: N/A

Table 5-523 HealthMonitor

Parameter	Type	Description
admin_state_up	Boolean	Definition: Specifies the administrative status of the health check. Range: • true: The health check function is enabled. • false: The health check function is disabled.
delay	Integer	Definition: Specifies the interval between health checks, in seconds. Range: 1 to 50
domain_name	String	Definition: Specifies the domain name that HTTP requests are sent to during the health check. Range: The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter.
expected_codes	String	Definition: Specifies the expected HTTP status code. Range: • 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	String	Definition: Specifies the HTTP method. Range: GET, HEAD, or POST
id	String	Specifies the health check ID. Default value: N/A
max_retries	Integer	Definition: Specifies the number of consecutive health checks when the health check result of a backend server changes from OFFLINE to ONLINE . Range: 1 to 10
max_retries_down	Integer	Definition: Specifies the number of consecutive health checks when the health check result of a backend server changes from ONLINE to OFFLINE . Range: 1 to 10

Parameter	Type	Description
monitor_port	Integer	Definition: Specifies the health check port. Range: 1 to 65535, or null (the port of a backend server will be used by default).
name	String	Definition: Specifies the health check name. Range: N/A
pools	Array of PoolRef objects	Specifies the IDs of the backend server groups for which the health check is configured. Only one ID will be returned. Range: N/A
project_id	String	Definition: Specifies the project ID. Range: N/A
timeout	Integer	Definition: Specifies the maximum time required for waiting for a response from the health check, in seconds. Range: N/A
type	String	Definition: Specifies the health check protocol. Range: The value can be TCP , UDP_CONNECT , HTTP , HTTPS , GRPC , or TLS .
url_path	String	Definition: Specifies the HTTP request path for the health check. The value must start with a slash (/), and the default value is /. Range: The value can contain letters, digits, hyphens (-), slashes (/), periods (.), percentage signs (%), question marks (?), pound signs (#), ampersand signs (&), and the extended character set: <code>_~!()*[]@\$^'+.</code>

Parameter	Type	Description
created_at	String	Definition: Specifies the creation time. Range: The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Note: This parameter 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	Definition: Specifies the update time. Range: The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Note: This parameter will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.

Table 5-524 PoolRef

Parameter	Type	Description
id	String	Definition: Specifies the backend server group ID. Range: N/A

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

Successful request.

```
{
  "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	Successful request.

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 5-525 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Table 5-526 Query Parameters

Parameter	Mandatory	Type	Description
marker	No	String	Definition: Specifies the ID of the last record on the previous page. Constraints: • This parameter must be used together with limit. • If the parameter is not specified, only resources on the first page are queried. • This parameter cannot be left blank or set to an invalid ID. Range: N/A Default value: N/A
limit	No	Integer	Definition: Specifies the number of records returned on each page. Constraints: N/A Range: 0 to 2000 Default value: 2000
page_reverse	No	Boolean	Definition: Specifies whether to use reverse query. Constraints: • This parameter must be used together with limit. • If page_reverse is set to true and you want to query the resources on the previous page, set the value of marker to the value of previous_marker. Range: • true: Query resources on the previous page. • false: Query resources on the next page. Default value: false

Parameter	Mandatory	Type	Description
id	No	Array of strings	Definition: Specifies the health check ID. Multiple IDs can be used for query in the format of <i>id=xxx&id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
monitor_port	No	Array of integers	Definition: Specifies the port used for the health check. Multiple ports can be used for query in the format of <i>monitor_port=xxx&monitor_port=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
domain_name	No	Array of strings	Definition: Specifies the domain name to which HTTP requests are sent during the health check. Multiple domain names can be used for query in the format of <i>domain_name=xxx&domain_name=xxx</i> . Constraints: N/A Range: The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter. Default value: N/A
name	No	Array of strings	Definition: Specifies the health check name. Multiple names can be used for query in the format of <i>name=xxx&name=xxx</i> . Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
delay	No	Array of integers	Definition: Specifies the interval between health checks, in seconds. Multiple intervals can be used for query in the format of <i>delay=xxx&delay=xxx</i>. Constraints: N/A Range: 1 to 50 Default value: N/A
max_retries	No	Array of integers	Definition: Specifies the number of consecutive health checks when the health check result of a backend server changes from OFFLINE to ONLINE. Multiple values can be used for query in the format of <i>max_retries=xxx&max_retries=xxx</i>. Constraints: N/A Range: 1 to 10 Default value: N/A
admin_state_up	No	Boolean	Definition: Specifies the administrative status of the health check. Constraints: N/A Range: • true: The health check function is enabled. • false: The health check function is disabled. Default value: N/A

Parameter	Mandatory	Type	Description
max_retries_down	No	Array of integers	Definition: Specifies the number of consecutive health checks when the health check result of a backend server changes from ONLINE to OFFLINE . Multiple values can be used for query in the format of <i>max_retries_down=xxx&max_retries_down=xxx</i> . Constraints: N/A Range: 1 to 10 Default value: N/A
timeout	No	Integer	Definition: Specifies the maximum time required for waiting for a response from the health check, in seconds. Constraints: N/A Range: N/A Default value: N/A
type	No	Array of strings	Definition: Specifies the health check protocol. Multiple protocols can be used for query in the format of <i>type=xxx&type=xxx</i> . Constraints: N/A Range: TCP, UDP_CONNECT, HTTP, HTTPS, TLS, or GRPC Default value: N/A

Parameter	Mandatory	Type	Description
expected_codes	No	Array of strings	Definition: Specifies the expected HTTP status code. Multiple status codes can be used for query in the format of <i>expected_codes=xxx&expected_codes=xxx</i> . Constraints: N/A Range: • 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 Default value: N/A
url_path	No	Array of strings	Definition: Specifies the HTTP request path for the health check. The value must start with a slash (/), and the default value is /. Multiple paths can be used for query in the format of <i>url_path=xxx&url_path=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
http_method	No	Array of strings	Definition: Specifies the HTTP method. Multiple methods can be used for query in the format of <i>http_method=xxx&http_method=xxx</i> . Constraints: N/A Range: GET, HEAD, or POST Default value: N/A

Parameter	Mandatory	Type	Description
enterprise_project_id	No	Array of strings	Definition: Specifies the ID of the enterprise project. Multiple values can be used for query in the format of: <i>enterprise_project_id=xxx&enterprise_project_id=xxx.</i> Constraints: • 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. Range: N/A Default value: N/A

Request Parameters

Table 5-527 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-528 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
page_info	PageInfo object	Definition: Specifies the pagination information.
healthmonitors	Array of HealthMonitor objects	Definition: Specifies the health check.

Table 5-529 PageInfo

Parameter	Type	Description
previous_marker	String	Definition: Specifies the ID of the first record in the pagination query result. If page_reverse is set to true , this parameter is used together to query resources on the previous page. Range: N/A
next_marker	String	Definition: Specifies the ID of the last record in the pagination query result. It is usually used to query resources on the next page. Range: N/A
current_count	Integer	Definition: Specifies the number of records returned on the current page. Range: N/A

Table 5-530 HealthMonitor

Parameter	Type	Description
admin_state_up	Boolean	Definition: Specifies the administrative status of the health check. Range: • true: The health check function is enabled. • false: The health check function is disabled.
delay	Integer	Definition: Specifies the interval between health checks, in seconds. Range: 1 to 50
domain_name	String	Definition: Specifies the domain name that HTTP requests are sent to during the health check. Range: The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter.
expected_codes	String	Definition: Specifies the expected HTTP status code. Range: • 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	String	Definition: Specifies the HTTP method. Range: GET, HEAD, or POST
id	String	Specifies the health check ID. Default value: N/A
max_retries	Integer	Definition: Specifies the number of consecutive health checks when the health check result of a backend server changes from OFFLINE to ONLINE . Range: 1 to 10
max_retries_down	Integer	Definition: Specifies the number of consecutive health checks when the health check result of a backend server changes from ONLINE to OFFLINE . Range: 1 to 10

Parameter	Type	Description
monitor_port	Integer	Definition: Specifies the health check port. Range: 1 to 65535, or null (the port of a backend server will be used by default).
name	String	Definition: Specifies the health check name. Range: N/A
pools	Array of PoolRef objects	Specifies the IDs of the backend server groups for which the health check is configured. Only one ID will be returned. Range: N/A
project_id	String	Definition: Specifies the project ID. Range: N/A
timeout	Integer	Definition: Specifies the maximum time required for waiting for a response from the health check, in seconds. Range: N/A
type	String	Definition: Specifies the health check protocol. Range: The value can be TCP , UDP_CONNECT , HTTP , HTTPS , GRPC , or TLS .
url_path	String	Definition: Specifies the HTTP request path for the health check. The value must start with a slash (/), and the default value is /. Range: The value can contain letters, digits, hyphens (-), slashes (/), periods (.), percentage signs (%), question marks (?), pound signs (#), ampersand signs (&), and the extended character set: <code>_~!()*[]@\$^'+.</code>

Parameter	Type	Description
created_at	String	Definition: Specifies the creation time. Range: The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Note: This parameter 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	Definition: Specifies the update time. Range: The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Note: This parameter will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.

Table 5-531 PoolRef

Parameter	Type	Description
id	String	Definition: Specifies the backend server group ID. Range: N/A

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

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudskgelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskgelb.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 5-532 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
healthmonitor_id	Yes	String	Definition: Specifies the health check ID. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-533 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-534 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
healthmonitor	HealthMonitor object	Definition: Specifies the health check.

Table 5-535 HealthMonitor

Parameter	Type	Description
admin_state_up	Boolean	Definition: Specifies the administrative status of the health check. Range: • true: The health check function is enabled. • false: The health check function is disabled.
delay	Integer	Definition: Specifies the interval between health checks, in seconds. Range: 1 to 50
domain_name	String	Definition: Specifies the domain name that HTTP requests are sent to during the health check. Range: The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter.
expected_codes	String	Definition: Specifies the expected HTTP status code. Range: • 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	String	Definition: Specifies the HTTP method. Range: GET, HEAD, or POST

Parameter	Type	Description
id	String	Specifies the health check ID. Default value: N/A
max_retries	Integer	Definition: Specifies the number of consecutive health checks when the health check result of a backend server changes from OFFLINE to ONLINE . Range: 1 to 10
max_retries_down	Integer	Definition: Specifies the number of consecutive health checks when the health check result of a backend server changes from ONLINE to OFFLINE . Range: 1 to 10
monitor_port	Integer	Definition: Specifies the health check port. Range: 1 to 65535, or null (the port of a backend server will be used by default).
name	String	Definition: Specifies the health check name. Range: N/A
pools	Array of PoolRef objects	Specifies the IDs of the backend server groups for which the health check is configured. Only one ID will be returned. Range: N/A
project_id	String	Definition: Specifies the project ID. Range: N/A
timeout	Integer	Definition: Specifies the maximum time required for waiting for a response from the health check, in seconds. Range: N/A
type	String	Definition: Specifies the health check protocol. Range: The value can be TCP , UDP_CONNECT , HTTP , HTTPS , GRPC , or TLS .

Parameter	Type	Description
url_path	String	Definition: Specifies the HTTP request path for the health check. The value must start with a slash (/), and the default value is /. Range: The value can contain letters, digits, hyphens (-), slashes (/), periods (.), percentage signs (%), question marks (?), pound signs (#), ampersand signs (&), and the extended character set: _~!()*[]@\$^'+.
created_at	String	Definition: Specifies the creation time. Range: The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Note: This parameter 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	Definition: Specifies the update time. Range: The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Note: This parameter will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.

Table 5-536 PoolRef

Parameter	Type	Description
id	String	Definition: Specifies the backend server group ID. Range: N/A

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.ElClientBuilder().
            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 5-537 Path Parameters

Parameter	Mandatory	Type	Description
healthmonitor_id	Yes	String	Definition: Specifies the health check ID. Constraints: N/A Range: N/A Default value: N/A
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-538 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-539 Request body parameters

Parameter	Mandatory	Type	Description
healthmonitor	Yes	UpdateHealthMonitorOption object	Definition: Specifies the health check. Constraints: N/A

Table 5-540 UpdateHealthMonitorOption

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Definition: Specifies the administrative status of the health check. Constraints: N/A Range: • true: The health check function is enabled. • false: The health check function is disabled. Default value: N/A
delay	No	Integer	Definition: Specifies the interval between health checks, in seconds. Constraints: N/A Range: 1 to 50 Default value: N/A

Parameter	Mandatory	Type	Description
domain_name	No	String	Definition: Specifies the domain name that HTTP requests are sent to during the health check. Constraints: This parameter is available only when type is set to HTTP or HTTPS. Range: 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. Default value: N/A
expected_codes	No	String	Definition: Specifies the expected HTTP status code. Constraints: This parameter will take effect only when type is set to HTTP, HTTPS or GRPC. Range: • 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 Default value: N/A
http_method	No	String	Definition: Specifies the HTTP method. Constraints: This parameter is available when type is set to HTTP or HTTPS. Range: GET, HEAD, or POST Default value: GET

Parameter	Mandatory	Type	Description
max_retries	No	Integer	Definition: Specifies the number of consecutive health checks when the health check result of a backend server changes from OFFLINE to ONLINE . Constraints: N/A Range: 1 to 10 Default value: N/A
max_retries_down	No	Integer	Definition: Specifies the number of consecutive health checks when the health check result of a backend server changes from ONLINE to OFFLINE . Constraints: N/A Range: 1 to 10 Default value: N/A
monitor_port	No	Integer	Definition: Specifies the health check port. Constraints: N/A Range: 1 to 65535, or null (the port of a backend server will be used by default). Default value: N/A
name	No	String	Definition: Specifies the health check name. Constraints: N/A Range: N/A Default value: N/A
timeout	No	Integer	Definition: Specifies the maximum time required for waiting for a response from the health check, in seconds. Constraints: N/A Range: It is recommended that you set the value less than that of parameter delay . Default value: N/A

Parameter	Mandatory	Type	Description
url_path	No	String	Definition: Specifies the HTTP request path for the health check. The value must start with a slash (/), and the default value is /. Constraints: This parameter is available only when type is set to HTTP or HTTPS. Range: The value can contain letters, digits, hyphens (-), slashes (/), periods (.), percentage signs (%), question marks (?), pound signs (#), ampersand signs (&), and the extended character set: _~!()*[]@\$^:'+,. Default value: N/A

Parameter	Mandatory	Type	Description
type	No	String	Definition: Specifies the health check protocol. Constraints: • 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. Range: The value can be TCP, UDP_CONNECT, HTTP, HTTPS, GRPC, or TLS. Default value: N/A

Response Parameters

Status code: 200

Table 5-541 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
healthmonitor	HealthMonitor object	Definition: Specifies the health check.

Table 5-542 HealthMonitor

Parameter	Type	Description
admin_state_up	Boolean	Definition: Specifies the administrative status of the health check. Range: • true: The health check function is enabled. • false: The health check function is disabled.
delay	Integer	Definition: Specifies the interval between health checks, in seconds. Range: 1 to 50
domain_name	String	Definition: Specifies the domain name that HTTP requests are sent to during the health check. Range: The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter.
expected_codes	String	Definition: Specifies the expected HTTP status code. Range: • 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	String	Definition: Specifies the HTTP method. Range: GET, HEAD, or POST

Parameter	Type	Description
id	String	Specifies the health check ID. Default value: N/A
max_retries	Integer	Definition: Specifies the number of consecutive health checks when the health check result of a backend server changes from OFFLINE to ONLINE . Range: 1 to 10
max_retries_down	Integer	Definition: Specifies the number of consecutive health checks when the health check result of a backend server changes from ONLINE to OFFLINE . Range: 1 to 10
monitor_port	Integer	Definition: Specifies the health check port. Range: 1 to 65535, or null (the port of a backend server will be used by default).
name	String	Definition: Specifies the health check name. Range: N/A
pools	Array of PoolRef objects	Specifies the IDs of the backend server groups for which the health check is configured. Only one ID will be returned. Range: N/A
project_id	String	Definition: Specifies the project ID. Range: N/A
timeout	Integer	Definition: Specifies the maximum time required for waiting for a response from the health check, in seconds. Range: N/A
type	String	Definition: Specifies the health check protocol. Range: The value can be TCP , UDP_CONNECT , HTTP , HTTPS , GRPC , or TLS .

Parameter	Type	Description
url_path	String	Definition: Specifies the HTTP request path for the health check. The value must start with a slash (/), and the default value is /. Range: The value can contain letters, digits, hyphens (-), slashes (/), periods (.), percentage signs (%), question marks (?), pound signs (#), ampersand signs (&), and the extended character set: _~!()*[]@\$^'+.
created_at	String	Definition: Specifies the creation time. Range: The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Note: This parameter 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	Definition: Specifies the update time. Range: The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Note: This parameter will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.

Table 5-543 PoolRef

Parameter	Type	Description
id	String	Definition: Specifies the backend server group ID. Range: N/A

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 5-544 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
healthmonitor_id	Yes	String	Definition: Specifies the health check ID. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-545 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 204

Successful request.

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.ElClientBuilder().
            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 5-546 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-547 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-548 Request body parameters

Parameter	Mandatory	Type	Description
l7policy	Yes	CreateL7PolicyOption object	Definition: Specifies the forwarding policy. Constraints: N/A

Table 5-549 CreateL7PolicyOption

Parameter	Mandatory	Type	Description
action	Yes	String	Definition: Specifies the action of the forwarding policy. Constraints: • 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. Range: • 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. Default value: N/A
admin_state_up	No	Boolean	Definition: Specifies the administrative status of the forwarding policy. Constraints: The value can only be true. Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
description	No	String	Definition: Provides supplementary information about the forwarding policy. Constraints: N/A Range: N/A Default value: N/A
listener_id	Yes	String	Definition: Specifies the ID of the listener with which the forwarding policy is associated. Constraints: • If action is set to REDIRECT_TO_POOL, the listener's protocol must be HTTP or HTTPS. • If action is set to REDIRECT_TO_LISTENER, the listener's protocol must be HTTP. Range: N/A Default value: N/A
name	No	String	Definition: Specifies the forwarding policy name. Constraints: N/A Range: N/A Default value: N/A
position	No	Integer	Definition: Specifies the priority of the forwarding policy. Constraints: The value cannot be updated. Range: N/A Default value: N/A This parameter is unsupported. Please do not use it.

Parameter	Mandatory	Type	Description
priority	No	Integer	Definition: Specifies the priority of the forwarding policy. A smaller value indicates a higher priority. Constraints: • The priority 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 set to false, 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 unsupported for shared load balancers. Range: • If action is set to REDIRECT_TO_LISTENER, the priority ranges from 0 to 10,000.

Parameter	Mandatory	Type	Description
			• If action is set to other values, the priority ranges from 1 to 10,000. Default value: • 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 there is no forwarding policy, the priority of a new forwarding policy will be 1 by default. – If the priority of an existing forwarding policy is the maximum value (10,000), the forwarding policy will fail to be created because the maximum value will be exceeded. In this case, specify a value or adjust the priorities of existing forwarding policies.
project_id	No	String	Definition: Specifies the ID of the project where the forwarding policy is used. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
redirect_listener_id	No	String	Definition: Specifies the ID of the listener to which requests are redirected. This parameter is mandatory when action is set to REDIRECT_TO_LISTENER. Constraints: • 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. Range: N/A Default value: N/A
redirect_pool_id	No	String	Definition: Specifies the ID of the backend server group to which requests will be forwarded. Constraints: • This parameter takes effect 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. Range: N/A Default value: N/A
redirect_url	No	String	Definition: Specifies the URL to which requests will be forwarded. Constraints: The value must be in the format of <i>protocol://host:port/path?query</i>. Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
redirect_url_config	No	CreateRedirectUrlConfig object	Definition: Specifies the URL to which requests are forwarded. Constraints: • 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. • 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. Otherwise, an error is reported. • For shared load balancers, this parameter is unsupported. If it is passed, an error will be returned.
redirect_pools_config	No	Array of CreateRedirectPoolsConfig objects	Definition: Specifies the backend server groups that the requests are forwarded to. Constraints: A maximum of five backend server groups can be configured for a forwarding policy.
redirect_pools_sticky_session_config	No	CreateRedirectPoolsStickySessionConfig object	Definition: 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 group. Constraints: This parameter is unsupported for shared load balancers. If it is passed, an error will be returned.

Parameter	Mandatory	Type	Description
fixed_response_config	No	CreateFixedResponseConfig object	Definition: Specifies the configuration of the page that will be returned. Constraints: • 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. • This parameter is mandatory when action is set to FIXED_RESPONSE. It cannot be specified if action is set to other values. • For shared load balancers, this parameter is unsupported. If it is passed, an error will be returned.
redirect_pools_extend_config	No	CreateRedirectPoolsExtendConfig object	Definition: Specifies the backend server group that requests are forwarded to. Constraints: This parameter takes effect only when action is set to REDIRECT_TO_POOL .

Parameter	Mandatory	Type	Description
rules	No	Array of CreateL7PolicyRuleOption objects	Definition: Lists the forwarding rules in the forwarding policy. Constraints: - 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. - The forwarding rule cannot be created when action is set to REDIRECT_TO_LISTENER.

Table 5-550 CreateRedirectUrlConfig

Parameter	Mandatory	Type	Description
protocol	No	String	Definition: Specifies the protocol for redirection. Constraints: N/A Range: HTTP HTTPS \${protocol}: indicates that the protocol in the request will be used. Default value: \${protocol}

Parameter	Mandatory	Type	Description
host	No	String	Definition: Specifies the name of the host that requests are redirected to. Constraints: N/A Range: The value can contain only letters, digits, hyphens (-), and periods (.) and must start with a letter or digit. Default value: <code>\${host}</code> , indicating that the host in the request will be used.
port	No	String	Definition: Specifies the port that requests are redirected to. Constraints: N/A Range: N/A Default value: <code>\${port}</code> , indicating that the port in the request will be used.
path	No	String	Definition: Specifies the path that requests are redirected to. Constraints: N/A Range: The value can contain only letters, digits, and special characters: <code>_~';@^-%#&\$. *+?,=!: \/() []{} </code> and must start with a slash (/). <code>\$1</code> , <code>\$2</code> , <code>\$3</code> , and all the way to <code>\$9</code> match the wildcard asterisk (*) in the requested URL. Default value: <code>\${path}</code> , indicating that the path in the request will be used.

Parameter	Mandatory	Type	Description
query	No	String	Definition: Specifies the query string set in the URL for redirection. The following is an example: In the URL https://www.example.com:8080/elb?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. In the example, \${query} indicates type=loadbalancer. Constraints: N/A Range: The value can contain only letters, digits, and the special characters: !\$&'()*+,-./:;=?@^_`. The letters are case-sensitive. \$1, \$2, \$3, and all the way to \$9 match the wildcard asterisk (*) in the requested URL. Default value: \${query}, indicating that the query string in the request will be used.
status_code	Yes	String	Definition: Specifies the status code returned after the requests are redirected. Constraints: N/A Range: • 301 • 302 • 303 • 307 • 308
insert_headers_config	No	CreateInsertHeadersConfig object	Definition: Specifies the headers you want to write into the request that matches the forwarding rule. Constraints: N/A

Parameter	Mandatory	Type	Description
remove_headers_config	No	CreateRemoveHeadersConfig object	Definition: Specifies the headers you want to remove from the request that matches the forwarding rule. Constraints: N/A

Table 5-551 CreateRedirectPoolsConfig

Parameter	Mandatory	Type	Description
pool_id	Yes	String	Definition: Specifies the backend server group ID. Constraints: N/A Range: N/A Default value: N/A
weight	No	String	Definition: Specifies the weight of the backend server group. Requests are routed to backend server groups based on their weights. The larger the weight is, the higher proportion of requests the backend server group receives. If the weight is set to 0, the backend server group will not accept new requests. Constraints: N/A Range: 0 to 100 Default value: 1

Table 5-552 CreateRedirectPoolsStickySessionConfig

Parameter	Mandatory	Type	Description
enable	No	Boolean	Definition: Specifies whether to enable sticky session for backend server groups configured in a forwarding policy. Constraints: N/A Range: The value can be true (enable this option) or false (disable this option). Default value: false , indicating that sticky session is disabled.
timeout	No	Integer	Definition: Specifies the stickiness duration, in minutes. Constraints: N/A Range: 1 to 1440, in minutes Default value: 1440

Table 5-553 CreateFixtedResponseConfig

Parameter	Mandatory	Type	Description
status_code	Yes	String	Definition: Specifies the HTTP status code. Constraints: N/A Range: 200-299, 400-499, 500-599 Default value: N/A
content_type	No	String	Definition: Specifies the format of the returned body. Constraints: N/A Range: • text/plain • text/css • text/html • application/javascript • application/json Default value: N/A

Parameter	Mandatory	Type	Description
message_body	No	String	Definition: Specifies the content of the response message body. Constraints: N/A Range: N/A Default value: N/A
insert_headers_config	No	CreateInsertHeadersConfig object	Definition: Specifies the headers you want to write into the request that matches the forwarding rule. Constraints: N/A
remove_headers_config	No	CreateRemoveHeadersConfig object	Definition: Specifies the headers you want to remove from the request that matches the forwarding rule. Constraints: N/A
traffic_limit_config	No	CreateTrafficLimitConfig object	Definition: Specifies how requests are limited. Constraints: N/A

Table 5-554 CreateRedirectPoolsExtendConfig

Parameter	Mandatory	Type	Description
rewrite_url_enable	No	Boolean	Definition: Specifies whether to set rewrite_url_enable to true .
rewrite_url_config	No	CreateRewriteUrlConfig object	Definition: Specifies the URL for the backend server group that requests are forwarded to. Constraints: This parameter takes effect only when action is set to REDIRECT_TO_POOL .
insert_headers_config	No	CreateInsertHeadersConfig object	Definition: Specifies the headers you want to write into the request that matches the forwarding rule. Constraints: N/A

Parameter	Mandatory	Type	Description
remove_headers_config	No	CreateRemoveHeadersConfig object	Definition: Specifies the headers you want to remove from the request that matches the forwarding rule. Constraints: N/A
traffic_limit_config	No	CreateTrafficLimitConfig object	Definition: Specifies how requests are limited. Constraints: N/A
cors_config	No	CreateCorsConfig object	Definition: Specifies the CORS configurations. Constraints: N/A
traffic_mirror_config	No	CreateTrafficMirrorConfig object	Definition: Specifies the traffic mirroring configuration. Constraints: N/A

Table 5-555 CreateRewriteUrlConfig

Parameter	Mandatory	Type	Description
host	No	String	Definition: Specifies the domain name of the host that requests are redirected to. Constraints: N/A Range: The value can contain letters, digits, hyphens (-), and periods (.), and must start with a letter or digit. Default value: <code>\${host}</code> , indicating that the host in the request will be used.

Parameter	Mandatory	Type	Description
path	No	String	Definition: Specifies the path that requests are redirected to. \$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 \$#. Constraints: N/A Range: The value must start with a slash (/) and can contain only letters, digits, and special characters: _~';@^-%#&\$.+?,=!: /() Default value: \${path}, indicating that the path in the request will be used.

Parameter	Mandatory	Type	Description
query	No	String	Definition: Specifies the query string set in the URL for redirection. \$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 \$# . Constraints: N/A Range: The value can contain only letters, digits, and the special characters: !\$&'()+,,-./:;=?@^_`. The letters are case-sensitive. Default value: \${query} , indicating that the query string in the request will be used.

Table 5-556 CreateInsertHeadersConfig

Parameter	Mandatory	Type	Description
configs	Yes	Array of CreateInsertHeaderConfig objects	Definition: Specifies the headers you want to write into the request that matches the forwarding rule. Constraints: N/A

Table 5-557 CreateInsertHeaderConfig

Parameter	Mandatory	Type	Description
key	Yes	String	Definition: Specifies the key of the header you want to write into the request that matches the forwarding rule. Constraints: The following cannot be used as a key. 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 Range: The value can contain 1 to 40 characters, including letters (case-insensitive), digits, hyphens (-), and underscores (_). Default value: N/A
value_type	Yes	String	Definition: Specifies the value type of the header. Constraints: N/A Range: USER_DEFINED , REFERENCE_HEADER , or SYSTEM_DEFINED Default value: N/A

Parameter	Mandatory	Type	Description
value	Yes	String	Definition: Specifies the value of the header. Constraints: 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 . Range: 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. Default value: N/A

Table 5-558 CreateRemoveHeadersConfig

Parameter	Mandatory	Type	Description
configs	Yes	Array of CreateRemoveHeaderConfig objects	Definition: Specifies the headers you want to remove from the request that matches the forwarding rule. Constraints: N/A

Table 5-559 CreateRemoveHeaderConfig

Parameter	Mandatory	Type	Description
key	Yes	String	Definition: Specifies the key of the header you want to remove from the request that matches the forwarding rule. Constraints: The following cannot be used as a key. 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 Range: The value can contain 1 to 40 characters, including letters (case-insensitive), digits, hyphens (-), and underscores (_). Default value: N/A

Table 5-560 CreateTrafficLimitConfig

Parameter	Mandatory	Type	Description
qps	No	Integer	Definition: Specifies the maximum number of queries per second (QPS). Constraints: N/A Range: 0 to 100000. Unit: count/s. 0 indicates that QPS is not limited. Default value: N/A

Parameter	Mandatory	Type	Description
per_source_ip_qps	No	Integer	Definition: Specifies the maximum number of queries per second (QPS) from a source IP address (single client). Constraints: • This parameter is not available for QUIC listeners. • The value can be 0 or null. • If qps is not set to 0, per_source_ip_qps must be specified a smaller value than qps. Range: 0 to 100000. Unit: count/s. 0 indicates that QPS is not limited. Default value: N/A
burst	No	Integer	Definition: Specifies the allowed burst queries if the number of queries exceeds the value specified for qps. If the number of burst queries exceeds the value specified for burst, 503 Service Unavailable will be returned to the client. Constraints: N/A Range: 0 to 100000. Unit: count/s. Default value: N/A

Table 5-561 CreateCorsConfig

Parameter	Mandatory	Type	Description
allow_origin	No	Array of strings	Definition: 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. Range: N/A Default value: N/A
allow_methods	No	Array of strings	Definition: Specifies the HTTP methods that the specified URLs can use to access cross-origin resources. Constraints: N/A Range: N/A Default value: N/A
allow_headers	No	Array of strings	Definition: Specifies the request headers that can be carried in CORS requests. Constraints: N/A Range: N/A Default value: N/A
expose_headers	No	Array of strings	Definition: Specifies the headers that can be exposed. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
allow_credentials	No	Boolean	Definition: Specifies whether to allow credentials in CORS requests. Constraints: N/A Range: • true: Credentials are allowed. • false: Credentials are not allowed. Default value: N/A
max_age	No	Long	Definition: Specifies the maximum duration a preflight request can be cached, in seconds. Constraints: N/A Range: -1 to 172800 Default value: N/A

Table 5-562 CreateTrafficMirrorConfig

Parameter	Mandatory	Type	Description
target_ids	No	Array of strings	Definition: Specifies the IDs of the backend server groups that traffic is mirrored to. Constraints: N/A Range: N/A Default value: N/A
mirror_request_body_enable	No	Boolean	Specifies whether to include the mirror request body. The default value is true . Constraints: N/A Range: N/A Default value: N/A

Table 5-563 CreateL7PolicyRuleOption

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Definition: Specifies the administrative status of the forwarding rule. Constraints: The value can only be true . Range: N/A Default value: N/A
type	Yes	String	Definition: Specifies the forwarding rule type. Constraints: 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. Range: • HOST_NAME: A domain name will be used for matching. • PATH: A URL will be used for matching. • METHOD: A request method will be used for matching. • HEADER: A request header will be used for matching. • QUERY_STRING: A query string will be used for matching. • SOURCE_IP: A source IP address will be used for matching. • COOKIE: A cookie will be used for matching. Default value: N/A

Parameter	Mandatory	Type	Description
compare_type	Yes	String	Definition: Specifies how requests are matched with the forwarding rule. Constraints: • 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. Range: • EQUAL_TO: exact match • REGEX: regular expression match • STARTS_WITH: prefix match Default value: N/A
invert	No	Boolean	Definition: Specifies whether reverse matching is supported. Constraints: N/A Range: true or false Default value: false This parameter is unsupported. Please do not use it.

Parameter	Mandatory	Type	Description
key	No	String	Definition: 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. Constraints: N/A Range: N/A Default value: N/A This parameter is unsupported. Please do not use it.

Parameter	Mandatory	Type	Description
value	Yes	String	Definition: Specifies the value of the match item. For example, if a domain name is used for matching, value is the domain name. Constraints: • This parameter takes effect only when conditions is left blank. • If type is set to HOST_NAME, the value can contain 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 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: <code>_~' ;@^-%#&\$. * + ?, = ! : \ / () [] { }</code> • 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. Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
conditions	No	Array of CreateRuleCondition objects	Definition: Specifies the conditions contained in a forwarding rule. Constraints: • This parameter takes effect only when enhance_l7policy_enable is set to true. • If conditions is set for a forwarding rule, the values of key and value are ignored. • All keys in the conditions of a rule must be the same, and the values must be unique.

Table 5-564 CreateRuleCondition

Parameter	Mandatory	Type	Description
key	No	String	Definition: Specifies the key of match item. Constraints: All keys in the conditions list in the same rule must be the same. Range: • 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. Each key 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 allowed. Default value: N/A

Parameter	Mandatory	Type	Description
value	Yes	String	Definition: Specifies the value of the match item. Constraints: • The key of each condition in a forwarding rule must be the same. • The value of each condition in a forwarding rule must be unique. Range: • If type is set to HOST_NAME, key is always an empty string and value indicates the domain name. Each value 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 always an empty string and value indicates the request path, which can contain 1 to 128 characters. If compare_type is set to STARTS_WITH or EQUAL_TO for a forwarding rule, the value must start with a slash (/) and can contain only letters, digits, and special characters: _~';@^-%#&\$. * +?,=!: \\V()[]{}. • 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 128 characters. Asterisks (*) and question marks (?) are

Parameter	Mandatory	Type	Description
			allowed, but spaces and double quotation marks are not allowed. An asterisk can match zero or more characters, and a question mark can match one 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 allowed. Asterisks (*) and question marks (?) are allowed. An asterisk can match zero or more characters, and a question mark can match one character. • If type is set to METHOD, key is always an empty string and 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 always an empty string and 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. Default value: N/A

Response Parameters

Status code: 201

Table 5-565 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Constraints: N/A Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-). Default value: N/A
l7policy	L7Policy object	Definition: Specifies the forwarding policy. Constraints: N/A

Table 5-566 L7Policy

Parameter	Type	Description
action	String	Definition: Specifies the action of the forwarding policy. Range: • 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.
admin_state_up	Boolean	Definition: Specifies the administrative status of the forwarding policy. Range: The value can only be true .
description	String	Definition: Provides supplementary information about the forwarding policy. Range: N/A
id	String	Definition: Specifies the forwarding policy ID. Range: N/A

Parameter	Type	Description
listener_id	String	Definition: Specifies the ID of the listener with which the forwarding policy is associated. Range: N/A
name	String	Definition: Specifies the forwarding policy name. Range: N/A
position	Integer	Definition: Specifies the priority of the forwarding policy. The priority cannot be updated. This parameter is unsupported. Please do not use it.
priority	Integer	Definition: Specifies the priority of the forwarding policy. A smaller value indicates a higher priority. Range: • 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.
project_id	String	Definition: Specifies the ID of the project where the forwarding policy is used. Range: N/A
provisioning_status	String	Definition: Specifies the provisioning status of the forwarding policy. Range: • ACTIVE (default): The forwarding policy is provisioned successfully. • ERROR: The forwarding policy has the same rule as another forwarding policy added to the same listener.
redirect_pool_id	String	Definition: Specifies the ID of the backend server group to which requests will be forwarded. Range: N/A
redirect_listener_id	String	Definition: Specifies the ID of the listener to which requests are redirected. Range: N/A

Parameter	Type	Description
redirect_url	String	Definition: Specifies the URL to which requests will be forwarded. Range: The value must be in the format of <i>protocol://host:port/path?query</i> . This parameter is unsupported. Please do not use it.
rules	Array of RuleRef objects	Definition: Lists the forwarding rules in the forwarding policy.
redirect_url_config	RedirectUrlConfig object	Definition: Specifies the URL to which requests are forwarded.
redirect_pools_config	Array of RedirectPoolsConfig objects	Definition: Specifies the backend server groups that the requests are forwarded to. This parameter takes effect only when enhance_l7policy_enable is set to true . If this parameter is specified and enhance_l7policy_enable is set to false , an error will be returned.
redirect_pools_sticky_session_config	RedirectPoolsStickySessionConfig object	Definition: 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 group.
redirect_pools_extend_config	RedirectPoolsExtendConfig object	Definition: Specifies the backend server group that requests are forwarded to.
fixed_response_config	FixedResponseConfig object	Definition: Specifies the configuration of the page that will be returned.
created_at	String	Definition: Specifies the creation time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format. Note: This parameter 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	Definition: Specifies the update time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format. Note: This parameter 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	Definition: Specifies the enterprise project ID. Range: N/A

Table 5-567 RuleRef

Parameter	Type	Description
id	String	Definition: Specifies the forwarding rule ID. Range: N/A

Table 5-568 RedirectUrlConfig

Parameter	Type	Description
protocol	String	Definition: Specifies the protocol for redirection. Range: • HTTP • HTTPS • \${protocol}: indicates that the protocol in the request will be used.
host	String	Definition: Specifies the name of the host that requests are redirected to. Range: The value can contain only letters, digits, hyphens (-), and periods (.) and must start with a letter or digit.
port	String	Definition: Specifies the port that requests are redirected to. Range: N/A

Parameter	Type	Description
path	String	Definition: Specifies the path that requests are redirected to. Range: The value can contain only letters, digits, and special characters: <code>_~';@^-%#&\$. *+?,=!: \\V() [] {}</code> and must start with a slash (/).
query	String	Definition: Specifies the query string set in the URL for redirection. The following is an example: In the URL https://www.example.com:8080/elb?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 . In the example, \${query} indicates type=loadbalancer . Range: The value can contain only letters, digits, and the special characters: <code>!\$&'()*+,-./:;=?@^_`</code> . The letters are case-sensitive. <code>\$1</code> , <code>\$2</code> , <code>\$3</code> , and all the way to <code>\$9</code> match the wildcard asterisk (*) in the requested URL.
status_code	String	Definition: Specifies the status code returned after the requests are redirected. Range: • 301 • 302 • 303 • 307 • 308
insert_headers_config	InsertHeadersConfig object	Definition: Specifies the headers you want to write into the request that matches the forwarding rule.
remove_headers_config	RemoveHeadersConfig object	Definition: Specifies the headers you want to remove from the request that matches the forwarding rule.

Table 5-569 RedirectPoolsConfig

Parameter	Type	Description
pool_id	String	Definition: Specifies the backend server group ID. Range: N/A
weight	Integer	Definition: Specifies the weight of the backend server group. Requests are routed to backend server groups based on their weights. The larger the weight is, the higher proportion of requests the backend server group receives. If the weight is set to 0, the backend server group will not accept new requests. Range: 0 to 100

Table 5-570 RedirectPoolsStickySessionConfig

Parameter	Type	Description
enable	Boolean	Definition: Specifies whether to enable sticky session for backend server groups configured in a forwarding policy. Default value: false , indicating that sticky session is disabled.
timeout	Integer	Definition: Specifies the stickiness duration, in minutes. Range: 1 to 1440

Table 5-571 RedirectPoolsExtendConfig

Parameter	Type	Description
rewrite_url_enable	Boolean	Definition: Specifies whether to set rewrite_url_enable to true . Range: The value can be true (enable this option) or false (disable this option).
rewrite_url_config	RewriteUrlConfig object	Definition: Specifies the URL for the backend server group that requests are forwarded to.

Parameter	Type	Description
insert_headers_config	InsertHeadersConfig object	Definition: Specifies the headers you want to write into the request that matches the forwarding rule.
remove_headers_config	RemoveHeadersConfig object	Definition: Specifies the headers you want to remove from the request that matches the forwarding rule.
traffic_limit_config	TrafficLimitConfig object	Definition: Specifies how requests are limited.
cors_config	CorsConfig object	Definition: Specifies the CORS configurations.
traffic_mirror_config	TrafficMirrorConfig object	Definition: Specifies the traffic mirroring configuration.

Table 5-572 RewriteUrlConfig

Parameter	Type	Description
host	String	Definition: Specifies the domain name of the host that requests are redirected to. Range: The value can contain letters, digits, hyphens (-), and periods (.), and must start with a letter or digit.
path	String	Definition: Specifies the path that requests are redirected to. \$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 \$# . Range: The value must start with a slash (/) and can contain only letters, digits, and special characters: <code>_~';@^-%#&\$.+?,:! /()</code>

Parameter	Type	Description
query	String	Definition: Specifies the query string set in the URL for redirection. \$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 \$# . Range: The value can contain only letters, digits, and the special characters: !\$&'()+,-./:;=?@^_`. The letters are case-sensitive.

Table 5-573 CorsConfig

Parameter	Type	Description
allow_origin	Array of strings	Definition: 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	Definition: Specifies the HTTP methods that the specified URLs can use to access cross-origin resources. Range: N/A
allow_headers	Array of strings	Definition: Specifies the request headers that can be carried in CORS requests. Range: N/A

Parameter	Type	Description
expose_headers	Array of strings	Definition: Specifies the headers that can be exposed. Range: N/A
allow_credentials	Boolean	Definition: Specifies whether to allow credentials in CORS requests. Range: • true: Credentials are allowed. • false: Credentials are not allowed.
max_age	Long	Definition: Specifies the maximum duration a preflight request can be cached, in seconds. Range: -1 to 172800

Table 5-574 TrafficMirrorConfig

Parameter	Type	Description
target_ids	Array of strings	Definition: Specifies the IDs of the backend server groups that traffic is mirrored to. Range: N/A
mirror_request_body_enable	Boolean	Specifies whether to include the mirror request body. The default value is true . Range: N/A

Table 5-575 FixedResponseConfig

Parameter	Type	Description
status_code	String	Definition: Specifies the HTTP status code. Range: 200-299, 400-499, 500-599
content_type	String	Definition: Specifies the format of the returned body. Range: • text/plain • text/css • text/html • application/javascript • application/json

Parameter	Type	Description
message_body	String	Definition: Specifies the content of the response message body. Range: N/A
insert_headers_config	InsertHeadersConfig object	Definition: Specifies the headers you want to write into the request that matches the forwarding rule.
remove_headers_config	RemoveHeadersConfig object	Definition: Specifies the headers you want to remove from the request that matches the forwarding rule.
traffic_limit_config	TrafficLimitConfig object	Definition: Specifies how requests are limited.

Table 5-576 InsertHeadersConfig

Parameter	Type	Description
configs	Array of InsertHeaderConfig objects	Definition: Specifies the headers you want to write into the request that matches the forwarding rule. Constraints: N/A

Table 5-577 InsertHeaderConfig

Parameter	Type	Description
key	String	Definition: Specifies the key of the header you want to write into the request that matches the forwarding rule. Range: The value can contain 1 to 40 characters, including letters (case-insensitive), digits, hyphens (-), and underscores (_).
value_type	String	Definition: Specifies the value type of the header. Range: USER_DEFINED , REFERENCE_HEADER , or SYSTEM_DEFINED

Parameter	Type	Description
value	String	Definition: Specifies the value of the header. Range: 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 5-578 RemoveHeadersConfig

Parameter	Type	Description
configs	Array of RemoveHeaderConfig objects	Definition: Specifies the headers you want to remove from the request that matches the forwarding rule. Constraints: N/A

Table 5-579 RemoveHeaderConfig

Parameter	Type	Description
key	String	Definition: Specifies the key of the header you want to remove from the request that matches the forwarding rule. Range: The value can contain 1 to 40 characters, including letters (case-insensitive), digits, hyphens (-), and underscores (_).

Table 5-580 TrafficLimitConfig

Parameter	Type	Description
qps	Integer	Definition: Specifies the maximum number of queries per second (QPS). Range: 0 to 100000. Unit: count/s. 0 indicates that QPS is not limited.

Parameter	Type	Description
per_source_ip_qps	Integer	Definition: Specifies the maximum number of queries per second (QPS) from a source IP address (single client). Range: 0 to 100000. Unit: count/s. 0 indicates that QPS is not limited.
burst	Integer	Definition: Specifies the allowed burst queries if the number of queries exceeds the value specified for qps . If the number of burst queries exceeds the value specified for burst , 503 Service Unavailable will be returned to the client. Range: 0 to 100000. Unit: count/s.

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

Successful request.

```
{
  "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	Successful request.

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 5-581 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Table 5-582 Query Parameters

Parameter	Mandatory	Type	Description
marker	No	String	Definition: Specifies the ID of the last record on the previous page. Constraints: • This parameter must be used together with limit. • If the parameter is not specified, only resources on the first page are queried. • This parameter cannot be left blank or set to an invalid ID. Range: N/A Default value: N/A
limit	No	Integer	Definition: Specifies the number of records returned on each page. Constraints: N/A Range: 0 to 2000 Default value: 2000
page_reverse	No	Boolean	Definition: Specifies whether to use reverse query. Constraints: • This parameter must be used together with limit. • If page_reverse is set to true and you want to query the resources on the previous page, set the value of marker to the value of previous_marker. Range: • true: Query resources on the previous page. • false: Query resources on the next page. Default value: false

Parameter	Mandatory	Type	Description
enterprise_project_id	No	Array of strings	Definition: Specifies the ID of the enterprise project. Multiple values can be used for query in the format of: <i>enterprise_project_id=xxx&enterprise_project_id=xxx.</i> Constraints: • 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. Range: N/A Default value: N/A
id	No	Array of strings	Definition: Specifies the forwarding policy ID. Multiple IDs can be used for query in the format of <i>id=xxx&id=xxx.</i> Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
name	No	Array of strings	Definition: Specifies the forwarding policy name. Multiple names can be used for query in the format of <i>name=xxx&name=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
description	No	Array of strings	Definition: Provides supplementary information about the forwarding policy. Multiple descriptions can be used for query in the format of <i>description=xxx&description=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
admin_state_up	No	Boolean	Definition: Specifies the administrative status of the forwarding policy. Constraints: N/A Range: N/A Default value: N/A
listener_id	No	Array of strings	Definition: Specifies the ID of the listener with which the forwarding policy is associated. Multiple IDs can be used for query in the format of <i>listener_id=xxx&listener_id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
position	No	Array of integers	Definition: Specifies the priority of the forwarding policy. Multiple priorities can be used for query in the format of <i>position=xxx&position=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
action	No	Array of strings	Definition: Specifies the action of the forwarding policy. Multiple actions can be used for query in the format of <i>action=xxx&action=xxx</i> . Constraints: N/A Range: ● 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. Default value: N/A
redirect_url	No	Array of strings	Definition: Specifies the URL to which requests will be forwarded. Multiple URLs can be used for query in the format of <i>redirect_url=xxx&redirect_url=xx</i> . Constraints: N/A Range: N/A Default value: N/A This parameter is unsupported. Please do not use it.

Parameter	Mandatory	Type	Description
redirect_pool_id	No	Array of strings	Definition: Specifies the ID of the backend server group to which requests will be forwarded. Multiple IDs can be used for query in the format of <i>redirect_pool_id=xxx&redirect_pool_id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
redirect_listener_id	No	Array of strings	Definition: Specifies the ID of the listener to which requests are redirected. Multiple IDs can be used for query in the format of <i>redirect_listener_id=xxx&redirect_listener_id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
provisioning_status	No	Array of strings	Definition: Specifies the provisioning status of the forwarding policy. Multiple provisioning statuses can be used for query in the format of <i>provisioning_status=xxx&provisioning_status=xxx</i> . Constraints: N/A Range: ● ACTIVE: The forwarding policy is provisioned successfully. ● ERROR: The forwarding policy has the same rule as another forwarding policy added to the same listener. Default value: N/A

Parameter	Mandatory	Type	Description
display_all_rules	No	Boolean	Definition: Specifies whether to display details about the forwarding rules in the forwarding policy. Constraints: N/A Range: • true: Details about the forwarding rules are displayed. • false: Only the rule IDs are displayed. Default value: N/A
priority	No	Array of integers	Definition: Specifies the priority of the forwarding policy. A smaller value indicates a higher priority. Multiple priorities can be used for query in the format of <i>priority=xxx&priority=xxx</i> . Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-583 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-584 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
page_info	PageInfo object	Definition: Specifies the pagination information.
l7policies	Array of L7Policy objects	Definition: Lists the forwarding policies.

Table 5-585 PageInfo

Parameter	Type	Description
previous_marker	String	Definition: Specifies the ID of the first record in the pagination query result. If page_reverse is set to true , this parameter is used together to query resources on the previous page. Range: N/A
next_marker	String	Definition: Specifies the ID of the last record in the pagination query result. It is usually used to query resources on the next page. Range: N/A
current_count	Integer	Definition: Specifies the number of records returned on the current page. Range: N/A

Table 5-586 L7Policy

Parameter	Type	Description
action	String	Definition: Specifies the action of the forwarding policy. Range: • 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.
admin_state_up	Boolean	Definition: Specifies the administrative status of the forwarding policy. Range: The value can only be true .
description	String	Definition: Provides supplementary information about the forwarding policy. Range: N/A
id	String	Definition: Specifies the forwarding policy ID. Range: N/A
listener_id	String	Definition: Specifies the ID of the listener with which the forwarding policy is associated. Range: N/A
name	String	Definition: Specifies the forwarding policy name. Range: N/A
position	Integer	Definition: Specifies the priority of the forwarding policy. The priority cannot be updated. This parameter is unsupported. Please do not use it.

Parameter	Type	Description
priority	Integer	Definition: Specifies the priority of the forwarding policy. A smaller value indicates a higher priority. Range: - 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.
project_id	String	Definition: Specifies the ID of the project where the forwarding policy is used. Range: N/A
provisioning_status	String	Definition: Specifies the provisioning status of the forwarding policy. Range: ACTIVE (default): The forwarding policy is provisioned successfully. ERROR: The forwarding policy has the same rule as another forwarding policy added to the same listener.
redirect_pool_id	String	Definition: Specifies the ID of the backend server group to which requests will be forwarded. Range: N/A
redirect_listener_id	String	Definition: Specifies the ID of the listener to which requests are redirected. Range: N/A
redirect_url	String	Definition: Specifies the URL to which requests will be forwarded. Range: The value must be in the format of <i>protocol://host:port/path?query</i> . This parameter is unsupported. Please do not use it.
rules	Array of RuleRef objects	Definition: Lists the forwarding rules in the forwarding policy.
redirect_url_config	RedirectUrlConfig object	Definition: Specifies the URL to which requests are forwarded.

Parameter	Type	Description
redirect_pools_config	Array of RedirectPoolsConfig objects	Definition: Specifies the backend server groups that the requests are forwarded to. This parameter takes effect only when enhance_l7policy_enable is set to true . If this parameter is specified and enhance_l7policy_enable is set to false , an error will be returned.
redirect_pools_sticky_session_config	RedirectPoolsStickySessionConfig object	Definition: 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 group.
redirect_pools_extend_config	RedirectPoolsExtendConfig object	Definition: Specifies the backend server group that requests are forwarded to.
fixed_response_config	FixedResponseConfig object	Definition: Specifies the configuration of the page that will be returned.
created_at	String	Definition: Specifies the creation time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format. Note: This parameter 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	Definition: Specifies the update time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format. Note: This parameter 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	Definition: Specifies the enterprise project ID. Range: N/A

Table 5-587 RuleRef

Parameter	Type	Description
id	String	Definition: Specifies the forwarding rule ID. Range: N/A

Table 5-588 RedirectUrlConfig

Parameter	Type	Description
protocol	String	Definition: Specifies the protocol for redirection. Range: • HTTP • HTTPS • \${protocol}: indicates that the protocol in the request will be used.
host	String	Definition: Specifies the name of the host that requests are redirected to. Range: The value can contain only letters, digits, hyphens (-), and periods (.) and must start with a letter or digit.
port	String	Definition: Specifies the port that requests are redirected to. Range: N/A
path	String	Definition: Specifies the path that requests are redirected to. Range: The value can contain only letters, digits, and special characters: <code>_~'!;@^-%#&\$.*+?,=!: \\()/[]{}</code> and must start with a slash (/).

Parameter	Type	Description
query	String	Definition: Specifies the query string set in the URL for redirection. The following is an example: In the URL https://www.example.com:8080/elb?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 . In the example, \${query} indicates type=loadbalancer . Range: The value can contain only letters, digits, and the special characters: !\$&'()*+,-./:;=?@^_` . The letters are case-sensitive. \$1, \$2, \$3 , and all the way to \$9 match the wildcard asterisk (*) in the requested URL.
status_code	String	Definition: Specifies the status code returned after the requests are redirected. Range: • 301 • 302 • 303 • 307 • 308
insert_headers_config	InsertHeadersConfig object	Definition: Specifies the headers you want to write into the request that matches the forwarding rule.
remove_headers_config	RemoveHeadersConfig object	Definition: Specifies the headers you want to remove from the request that matches the forwarding rule.

Table 5-589 RedirectPoolsConfig

Parameter	Type	Description
pool_id	String	Definition: Specifies the backend server group ID. Range: N/A

Parameter	Type	Description
weight	Integer	Definition: Specifies the weight of the backend server group. Requests are routed to backend server groups based on their weights. The larger the weight is, the higher proportion of requests the backend server group receives. If the weight is set to 0, the backend server group will not accept new requests. Range: 0 to 100

Table 5-590 RedirectPoolsStickySessionConfig

Parameter	Type	Description
enable	Boolean	Definition: Specifies whether to enable sticky session for backend server groups configured in a forwarding policy. Default value: false , indicating that sticky session is disabled.
timeout	Integer	Definition: Specifies the stickiness duration, in minutes. Range: 1 to 1440

Table 5-591 RedirectPoolsExtendConfig

Parameter	Type	Description
rewrite_url_enable	Boolean	Definition: Specifies whether to set rewrite_url_enable to true . Range: The value can be true (enable this option) or false (disable this option).
rewrite_url_config	RewriteUrlConfig object	Definition: Specifies the URL for the backend server group that requests are forwarded to.
insert_headers_config	InsertHeadersConfig object	Definition: Specifies the headers you want to write into the request that matches the forwarding rule.
remove_headers_config	RemoveHeadersConfig object	Definition: Specifies the headers you want to remove from the request that matches the forwarding rule.

Parameter	Type	Description
traffic_limit_config	TrafficLimitConfig object	Definition: Specifies how requests are limited.
cors_config	CorsConfig object	Definition: Specifies the CORS configurations.
traffic_mirror_config	TrafficMirrorConfig object	Definition: Specifies the traffic mirroring configuration.

Table 5-592 RewriteUrlConfig

Parameter	Type	Description
host	String	Definition: Specifies the domain name of the host that requests are redirected to. Range: The value can contain letters, digits, hyphens (-), and periods (.), and must start with a letter or digit.
path	String	Definition: Specifies the path that requests are redirected to. \$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 \$# . Range: The value must start with a slash (/) and can contain only letters, digits, and special characters: _~';@^-%#&\$.+?,:! /()

Parameter	Type	Description
query	String	Definition: Specifies the query string set in the URL for redirection. \$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 \$# . Range: The value can contain only letters, digits, and the special characters: !\$&'()+,-./:;=?@^_`. The letters are case-sensitive.

Table 5-593 CorsConfig

Parameter	Type	Description
allow_origin	Array of strings	Definition: 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	Definition: Specifies the HTTP methods that the specified URLs can use to access cross-origin resources. Range: N/A
allow_headers	Array of strings	Definition: Specifies the request headers that can be carried in CORS requests. Range: N/A

Parameter	Type	Description
expose_headers	Array of strings	Definition: Specifies the headers that can be exposed. Range: N/A
allow_credentials	Boolean	Definition: Specifies whether to allow credentials in CORS requests. Range: • true: Credentials are allowed. • false: Credentials are not allowed.
max_age	Long	Definition: Specifies the maximum duration a preflight request can be cached, in seconds. Range: -1 to 172800

Table 5-594 TrafficMirrorConfig

Parameter	Type	Description
target_ids	Array of strings	Definition: Specifies the IDs of the backend server groups that traffic is mirrored to. Range: N/A
mirror_request_body_enable	Boolean	Specifies whether to include the mirror request body. The default value is true . Range: N/A

Table 5-595 FixedResponseConfig

Parameter	Type	Description
status_code	String	Definition: Specifies the HTTP status code. Range: 200-299, 400-499, 500-599
content_type	String	Definition: Specifies the format of the returned body. Range: • text/plain • text/css • text/html • application/javascript • application/json

Parameter	Type	Description
message_body	String	Definition: Specifies the content of the response message body. Range: N/A
insert_headers_config	InsertHeadersConfig object	Definition: Specifies the headers you want to write into the request that matches the forwarding rule.
remove_headers_config	RemoveHeadersConfig object	Definition: Specifies the headers you want to remove from the request that matches the forwarding rule.
traffic_limit_config	TrafficLimitConfig object	Definition: Specifies how requests are limited.

Table 5-596 InsertHeadersConfig

Parameter	Type	Description
configs	Array of InsertHeaderConfig objects	Definition: Specifies the headers you want to write into the request that matches the forwarding rule. Constraints: N/A

Table 5-597 InsertHeaderConfig

Parameter	Type	Description
key	String	Definition: Specifies the key of the header you want to write into the request that matches the forwarding rule. Range: The value can contain 1 to 40 characters, including letters (case-insensitive), digits, hyphens (-), and underscores (_).
value_type	String	Definition: Specifies the value type of the header. Range: USER_DEFINED , REFERENCE_HEADER , or SYSTEM_DEFINED

Parameter	Type	Description
value	String	Definition: Specifies the value of the header. Range: 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	Definition: Specifies the headers you want to remove from the request that matches the forwarding rule. Constraints: N/A

Table 5-599 RemoveHeaderConfig

Parameter	Type	Description
key	String	Definition: Specifies the key of the header you want to remove from the request that matches the forwarding rule. Range: The value can contain 1 to 40 characters, including letters (case-insensitive), digits, hyphens (-), and underscores (_).

Table 5-600 TrafficLimitConfig

Parameter	Type	Description
qps	Integer	Definition: Specifies the maximum number of queries per second (QPS). Range: 0 to 100000. Unit: count/s. 0 indicates that QPS is not limited.

Parameter	Type	Description
per_source_ip_qps	Integer	Definition: Specifies the maximum number of queries per second (QPS) from a source IP address (single client). Range: 0 to 100000. Unit: count/s. 0 indicates that QPS is not limited.
burst	Integer	Definition: Specifies the allowed burst queries if the number of queries exceeds the value specified for qps . If the number of burst queries exceeds the value specified for burst , 503 Service Unavailable will be returned to the client. Range: 0 to 100000. Unit: count/s.

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

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from 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 5-601 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
l7policy_id	Yes	String	Definition: Specifies the forwarding policy ID. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-602 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-603 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
l7policy	L7Policy object	Definition: Specifies the forwarding policy.

Table 5-604 L7Policy

Parameter	Type	Description
action	String	Definition: Specifies the action of the forwarding policy. Range: • 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.
admin_state_up	Boolean	Definition: Specifies the administrative status of the forwarding policy. Range: The value can only be true .
description	String	Definition: Provides supplementary information about the forwarding policy. Range: N/A
id	String	Definition: Specifies the forwarding policy ID. Range: N/A
listener_id	String	Definition: Specifies the ID of the listener with which the forwarding policy is associated. Range: N/A

Parameter	Type	Description
name	String	Definition: Specifies the forwarding policy name. Range: N/A
position	Integer	Definition: Specifies the priority of the forwarding policy. The priority cannot be updated. This parameter is unsupported. Please do not use it.
priority	Integer	Definition: Specifies the priority of the forwarding policy. A smaller value indicates a higher priority. Range: • 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.
project_id	String	Definition: Specifies the ID of the project where the forwarding policy is used. Range: N/A
provisioning_status	String	Definition: Specifies the provisioning status of the forwarding policy. Range: • ACTIVE (default): The forwarding policy is provisioned successfully. • ERROR: The forwarding policy has the same rule as another forwarding policy added to the same listener.
redirect_pool_id	String	Definition: Specifies the ID of the backend server group to which requests will be forwarded. Range: N/A
redirect_listener_id	String	Definition: Specifies the ID of the listener to which requests are redirected. Range: N/A

Parameter	Type	Description
redirect_url	String	Definition: Specifies the URL to which requests will be forwarded. Range: The value must be in the format of <i>protocol://host:port/path?query</i> . This parameter is unsupported. Please do not use it.
rules	Array of RuleRef objects	Definition: Lists the forwarding rules in the forwarding policy.
redirect_url_config	RedirectUrlConfig object	Definition: Specifies the URL to which requests are forwarded.
redirect_pools_config	Array of RedirectPoolsConfig objects	Definition: Specifies the backend server groups that the requests are forwarded to. This parameter takes effect only when enhance_l7policy_enable is set to true . If this parameter is specified and enhance_l7policy_enable is set to false , an error will be returned.
redirect_pools_sticky_session_config	RedirectPoolsStickySessionConfig object	Definition: 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 group.
redirect_pools_extend_config	RedirectPoolsExtendConfig object	Definition: Specifies the backend server group that requests are forwarded to.
fixed_response_config	FixedResponseConfig object	Definition: Specifies the configuration of the page that will be returned.
created_at	String	Definition: Specifies the creation time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format. Note: This parameter 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	Definition: Specifies the update time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format. Note: This parameter 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	Definition: Specifies the enterprise project ID. Range: N/A

Table 5-605 RuleRef

Parameter	Type	Description
id	String	Definition: Specifies the forwarding rule ID. Range: N/A

Table 5-606 RedirectUrlConfig

Parameter	Type	Description
protocol	String	Definition: Specifies the protocol for redirection. Range: • HTTP • HTTPS • \${protocol}: indicates that the protocol in the request will be used.
host	String	Definition: Specifies the name of the host that requests are redirected to. Range: The value can contain only letters, digits, hyphens (-), and periods (.) and must start with a letter or digit.
port	String	Definition: Specifies the port that requests are redirected to. Range: N/A

Parameter	Type	Description
path	String	Definition: Specifies the path that requests are redirected to. Range: The value can contain only letters, digits, and special characters: <code>_~';@^-%#&\$. *+?,=!: \\V()[]{} </code> and must start with a slash (/).
query	String	Definition: Specifies the query string set in the URL for redirection. The following is an example: In the URL https://www.example.com:8080/elb?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 . In the example, \${query} indicates type=loadbalancer . Range: The value can contain only letters, digits, and the special characters: <code>!\$&'()*+,-./:;=?@^_` </code> . The letters are case-sensitive. <code>\$1, \$2, \$3, </code> and all the way to <code>\$9 </code> match the wildcard asterisk (*) in the requested URL.
status_code	String	Definition: Specifies the status code returned after the requests are redirected. Range: • 301 • 302 • 303 • 307 • 308
insert_headers_config	InsertHeadersConfig object	Definition: Specifies the headers you want to write into the request that matches the forwarding rule.
remove_headers_config	RemoveHeadersConfig object	Definition: Specifies the headers you want to remove from the request that matches the forwarding rule.

Table 5-607 RedirectPoolsConfig

Parameter	Type	Description
pool_id	String	Definition: Specifies the backend server group ID. Range: N/A
weight	Integer	Definition: Specifies the weight of the backend server group. Requests are routed to backend server groups based on their weights. The larger the weight is, the higher proportion of requests the backend server group receives. If the weight is set to 0, the backend server group will not accept new requests. Range: 0 to 100

Table 5-608 RedirectPoolsStickySessionConfig

Parameter	Type	Description
enable	Boolean	Definition: Specifies whether to enable sticky session for backend server groups configured in a forwarding policy. Default value: false , indicating that sticky session is disabled.
timeout	Integer	Definition: Specifies the stickiness duration, in minutes. Range: 1 to 1440

Table 5-609 RedirectPoolsExtendConfig

Parameter	Type	Description
rewrite_url_enable	Boolean	Definition: Specifies whether to set rewrite_url_enable to true . Range: The value can be true (enable this option) or false (disable this option).
rewrite_url_config	RewriteUrlConfig object	Definition: Specifies the URL for the backend server group that requests are forwarded to.

Parameter	Type	Description
insert_headers_config	InsertHeadersConfig object	Definition: Specifies the headers you want to write into the request that matches the forwarding rule.
remove_headers_config	RemoveHeadersConfig object	Definition: Specifies the headers you want to remove from the request that matches the forwarding rule.
traffic_limit_config	TrafficLimitConfig object	Definition: Specifies how requests are limited.
cors_config	CorsConfig object	Definition: Specifies the CORS configurations.
traffic_mirror_config	TrafficMirrorConfig object	Definition: Specifies the traffic mirroring configuration.

Table 5-610 RewriteUrlConfig

Parameter	Type	Description
host	String	Definition: Specifies the domain name of the host that requests are redirected to. Range: The value can contain letters, digits, hyphens (-), and periods (.), and must start with a letter or digit.
path	String	Definition: Specifies the path that requests are redirected to. \$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 \$# . Range: The value must start with a slash (/) and can contain only letters, digits, and special characters: _~';@^-%#&\$.+?,:! /()

Parameter	Type	Description
query	String	Definition: Specifies the query string set in the URL for redirection. \$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 \$# . Range: The value can contain only letters, digits, and the special characters: !\$&'()+,-./:;=?@^_`. The letters are case-sensitive.

Table 5-611 CorsConfig

Parameter	Type	Description
allow_origin	Array of strings	Definition: 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	Definition: Specifies the HTTP methods that the specified URLs can use to access cross-origin resources. Range: N/A
allow_headers	Array of strings	Definition: Specifies the request headers that can be carried in CORS requests. Range: N/A

Parameter	Type	Description
expose_headers	Array of strings	Definition: Specifies the headers that can be exposed. Range: N/A
allow_credentials	Boolean	Definition: Specifies whether to allow credentials in CORS requests. Range: • true: Credentials are allowed. • false: Credentials are not allowed.
max_age	Long	Definition: Specifies the maximum duration a preflight request can be cached, in seconds. Range: -1 to 172800

Table 5-612 TrafficMirrorConfig

Parameter	Type	Description
target_ids	Array of strings	Definition: Specifies the IDs of the backend server groups that traffic is mirrored to. Range: N/A
mirror_request_body_enable	Boolean	Specifies whether to include the mirror request body. The default value is true . Range: N/A

Table 5-613 FixedResponseConfig

Parameter	Type	Description
status_code	String	Definition: Specifies the HTTP status code. Range: 200-299, 400-499, 500-599
content_type	String	Definition: Specifies the format of the returned body. Range: • text/plain • text/css • text/html • application/javascript • application/json

Parameter	Type	Description
message_body	String	Definition: Specifies the content of the response message body. Range: N/A
insert_headers_config	InsertHeadersConfig object	Definition: Specifies the headers you want to write into the request that matches the forwarding rule.
remove_headers_config	RemoveHeadersConfig object	Definition: Specifies the headers you want to remove from the request that matches the forwarding rule.
traffic_limit_config	TrafficLimitConfig object	Definition: Specifies how requests are limited.

Table 5-614 InsertHeadersConfig

Parameter	Type	Description
configs	Array of InsertHeaderConfig objects	Definition: Specifies the headers you want to write into the request that matches the forwarding rule. Constraints: N/A

Table 5-615 InsertHeaderConfig

Parameter	Type	Description
key	String	Definition: Specifies the key of the header you want to write into the request that matches the forwarding rule. Range: The value can contain 1 to 40 characters, including letters (case-insensitive), digits, hyphens (-), and underscores (_).
value_type	String	Definition: Specifies the value type of the header. Range: USER_DEFINED , REFERENCE_HEADER , or SYSTEM_DEFINED

Parameter	Type	Description
value	String	Definition: Specifies the value of the header. Range: 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 5-616 RemoveHeadersConfig

Parameter	Type	Description
configs	Array of RemoveHeaderConfig objects	Definition: Specifies the headers you want to remove from the request that matches the forwarding rule. Constraints: N/A

Table 5-617 RemoveHeaderConfig

Parameter	Type	Description
key	String	Definition: Specifies the key of the header you want to remove from the request that matches the forwarding rule. Range: The value can contain 1 to 40 characters, including letters (case-insensitive), digits, hyphens (-), and underscores (_).

Table 5-618 TrafficLimitConfig

Parameter	Type	Description
qps	Integer	Definition: Specifies the maximum number of queries per second (QPS). Range: 0 to 100000. Unit: count/s. 0 indicates that QPS is not limited.

Parameter	Type	Description
per_source_ip_qps	Integer	Definition: Specifies the maximum number of queries per second (QPS) from a source IP address (single client). Range: 0 to 100000. Unit: count/s. 0 indicates that QPS is not limited.
burst	Integer	Definition: Specifies the allowed burst queries if the number of queries exceeds the value specified for qps . If the number of burst queries exceeds the value specified for burst , 503 Service Unavailable will be returned to the client. Range: 0 to 100000. Unit: count/s.

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 = "{projectId}";

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

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudskelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskelb.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.ElClientBuilder().
            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 5-619 Path Parameters

Parameter	Mandatory	Type	Description
l7policy_id	Yes	String	Definition: Specifies the forwarding policy ID. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-620 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-621 Request body parameters

Parameter	Mandatory	Type	Description
l7policy	Yes	UpdateL7PolicyOption object	Definition: Specifies the forwarding policy. Constraints: N/A

Table 5-622 UpdateL7PolicyOption

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Definition: Specifies the administrative status of the forwarding policy. Constraints: The value can only be true . Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
description	No	String	Definition: Provides supplementary information about the forwarding policy. Constraints: N/A Range: N/A Default value: N/A
name	No	String	Definition: Specifies the forwarding policy name. Constraints: N/A Range: N/A Default value: N/A
redirect_listener_id	No	String	Definition: Specifies the ID of the listener to which requests are redirected. Constraints: • If action is set to REDIRECT_TO_LISTENER, this parameter cannot be updated to an empty value or be null. • 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. Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
redirect_pool_id	No	String	Definition: Specifies the ID of the backend server group to which requests will be forwarded. Constraints: • 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 to an empty value and cannot be null. • If this parameter is specified when action is set to REDIRECT_TO_LISTENER, an error will be reported. Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
redirect_pools_config	No	Array of UpdateRedirectPoolsConfig objects	Definition: Specifies the new weights of backend server group that the requests are forwarded to. This parameter takes effect only when enhance_l7policy_enable is set to true. If this parameter is specified and enhance_l7policy_enable is set to false, an error will be returned. Constraints: • If action is set to REDIRECT_TO_POOL, specify either redirect_pool_id or redirect_pools_config. If both are specified, only redirect_pools_config takes effect. • If action is set to REDIRECT_TO_LISTENER or REDIRECT_TO_URL and this parameter is specified, an error will be returned. • A maximum of five backend server groups can be configured for a forwarding policy. Each backend server group must be unique. • All backend server groups will be overwritten, and the backend server groups that are not included in the request parameter in the request body will be removed. This parameter is unsupported for shared load balancers. If it is passed, an error will be returned.

Parameter	Mandatory	Type	Description
redirect_pools_sticky_session_config	No	UpdateRedirectPoolsStickySessionConfig object	Definition: 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 group. Constraints: This parameter is unsupported for shared load balancers. If it is passed, an error will be returned.
redirect_url_config	No	UpdateRedirectUrlConfig object	Definition: Specifies the URL to which requests are forwarded. Constraints: • 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. • 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. Otherwise, an error is reported. • For shared load balancers, this parameter is unsupported. If it is passed, an error will be returned.

Parameter	Mandatory	Type	Description
fixed_response_config	No	UpdateFixedResponseConfig object	Definition: Specifies the configuration of the page that will be returned. Constraints: • 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. • This parameter is mandatory when action is set to FIXED_RESPONSE. It cannot be specified if action is set to other values. • For shared load balancers, this parameter is unsupported. If it is passed, an error will be returned.
redirect_pools_extend_config	No	UpdateRedirectPoolsExtendConfig object	Definition: Specifies the backend server group that requests are forwarded to. Constraints: This parameter takes effect only when action is set to REDIRECT_TO_POOL .
rules	No	Array of CreateRuleOption objects	Definition: Lists the forwarding rules in the forwarding policy. Constraints: • 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	Definition: Specifies the priority of the forwarding policy. A smaller value indicates a higher priority. Constraints: • The priority 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 set to false, 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 unsupported for shared load balancers. Range: • If action is set to REDIRECT_TO_LISTENER, the priority ranges from 0 to 10,000.

Parameter	Mandatory	Type	Description
			• If action is set to other values, the priority ranges from 1 to 10,000. Default value: • 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 there is no forwarding policy, the priority of a new forwarding policy will be 1 by default. – If the priority of an existing forwarding policy is the maximum value (10,000), the forwarding policy will fail to be created because the maximum value will be exceeded. In this case, specify a value or adjust the priorities of existing forwarding policies.

Table 5-623 UpdateRedirectPoolsConfig

Parameter	Mandatory	Type	Description
pool_id	Yes	String	Definition: Specifies the backend server group ID. Constraints: N/A Range: N/A Default value: N/A
weight	No	String	Definition: Specifies the weight of the backend server group. Requests are routed to backend server groups based on their weights. The larger the weight is, the higher proportion of requests the backend server group receives. If the weight is set to 0, the backend server group will not accept new requests. Constraints: N/A Range: 0 to 100 Default value: N/A

Table 5-624 UpdateRedirectPoolsStickySessionConfig

Parameter	Mandatory	Type	Description
enable	No	Boolean	Definition: Specifies whether to enable sticky session for backend server groups configured in a forwarding policy. Constraints: N/A Range: N/A Default value: false, indicating that sticky session is disabled.
timeout	No	Integer	Definition: Specifies the stickiness duration, in minutes. Constraints: N/A Range: 1 to 1440 Default value: 1440

Table 5-625 UpdateRedirectUrlConfig

Parameter	Mandatory	Type	Description
protocol	No	String	Definition: Specifies the protocol for redirection. Constraints: N/A Range: • HTTP • HTTPS • \${protocol}: indicates that the protocol in the request will be used. Default value: N/A
host	No	String	Definition: Specifies the name of the host that requests are redirected to. Constraints: N/A Range: The value can contain only letters, digits, hyphens (-), and periods (.) and must start with a letter or digit. Default value: \${host} , indicating that the host in the request will be used.
port	No	String	Definition: Specifies the port that requests are redirected to. Constraints: N/A Range: N/A Default value: \${port} , indicating that the port in the request will be used.
path	No	String	Definition: Specifies the path that requests are redirected to. Constraints: N/A Range: The value can contain only letters, digits, and special characters: <code>_~';@^-%#&\$. *+?,=!: \/() []{} </code> and must start with a slash (/). Default value: \${path} , indicating that the path in the request will be used.

Parameter	Mandatory	Type	Description
query	No	String	Definition: Specifies the query string set in the URL for redirection. The following is an example: In the URL https://www.example.com:8080/elb?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. In the example, \${query} indicates type=loadbalancer. Constraints: N/A Range: The value can contain only letters, digits, and the special characters: !\$&'()*+,-./:;=?@^_`. The letters are case-sensitive. \$1, \$2, \$3, and all the way to \$9 match the wildcard asterisk (*) in the requested URL. Default value: \${query}, indicating that the query string in the request will be used.
status_code	No	String	Definition: Specifies the status code returned after the requests are redirected. Constraints: N/A Range: • 301 • 302 • 303 • 307 • 308 Default value: N/A
insert_headers_config	No	UpdateInsertHeadersConfig object	Definition: Specifies the headers you want to write into the request that matches the forwarding rule. Constraints: N/A

Parameter	Mandatory	Type	Description
remove_headers_config	No	UpdateRemoveHeadersConfig object	Definition: Specifies the headers you want to remove from the request that matches the forwarding rule. Default value: N/A

Table 5-626 UpdateFixedResponseConfig

Parameter	Mandatory	Type	Description
status_code	No	String	Definition: Specifies the HTTP status code. Constraints: N/A Range: 200-299, 400-499, 500-599 Default value: N/A
content_type	No	String	Definition: Specifies the format of the returned body. Constraints: N/A Range: • text/plain • text/css • text/html • application/javascript • application/json Default value: application/json
message_body	No	String	Definition: Specifies the content of the response message body. Constraints: N/A Range: N/A Default value: N/A
insert_headers_config	No	UpdateInsertHeadersConfig object	Definition: Specifies the headers you want to write into the request that matches the forwarding rule. Constraints: N/A

Parameter	Mandatory	Type	Description
remove_headers_config	No	UpdateRemoveHeadersConfig object	Definition: Specifies the headers you want to remove from the request that matches the forwarding rule. Default value: N/A
traffic_limit_config	No	UpdateTrafficLimitConfig object	Definition: Specifies how requests are limited. Constraints: N/A

Table 5-627 UpdateRedirectPoolsExtendConfig

Parameter	Mandatory	Type	Description
rewrite_url_enable	No	Boolean	Definition: Specifies whether to set rewrite_url_enable to true . Constraints: N/A Range: The value can be true (enable this option) or false (disable this option). Default value: N/A
rewrite_url_config	No	UpdateRewriteUrlConfig object	Definition: Specifies the URL for the backend server group that requests are forwarded to. Constraints: This parameter takes effect only when action is set to REDIRECT_TO_POOL .
insert_headers_config	No	UpdateInsertHeadersConfig object	Definition: Specifies the headers you want to write into the request that matches the forwarding rule. Constraints: N/A
remove_headers_config	No	UpdateRemoveHeadersConfig object	Definition: Specifies the headers you want to remove from the request that matches the forwarding rule. Default value: N/A
traffic_limit_config	No	UpdateTrafficLimitConfig object	Definition: Specifies how requests are limited. Constraints: N/A

Parameter	Mandatory	Type	Description
cors_config	No	CreateCorsConfig object	Definition: Specifies the CORS configurations. Constraints: N/A
traffic_mirror_config	No	CreateTrafficMirrorConfig object	Definition: Specifies the traffic mirroring configuration. Constraints: N/A

Table 5-628 UpdateRewriteUrlConfig

Parameter	Mandatory	Type	Description
host	No	String	Definition: Specifies the domain name of the host that requests are redirected to. Constraints: N/A Range: The value can contain letters, digits, hyphens (-), and periods (.), and must start with a letter or digit. Default value: N/A
path	No	String	Definition: Specifies the path that requests are redirected to. \$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 \$# . Constraints: N/A Range: The value must start with a slash (/) and can contain only letters, digits, and special characters: _~';@^-%#&\$.+?,=!: /() Default value: N/A

Parameter	Mandatory	Type	Description
query	No	String	Definition: Specifies the query string set in the URL for redirection. \$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 \$# . Constraints: N/A Range: The value can contain only letters, digits, and the special characters: !&'() +,-./:;=?@^_`. The letters are case-sensitive. Default value: N/A

Table 5-629 UpdateInsertHeadersConfig

Parameter	Mandatory	Type	Description
configs	Yes	Array of UpdateInsertHeaderConfig objects	Definition: Specifies the headers you want to write into the request that matches the forwarding rule. Constraints: N/A

Table 5-630 UpdateInsertHeaderConfig

Parameter	Mandatory	Type	Description
key	Yes	String	Definition: Specifies the key of the header you want to write into the request that matches the forwarding rule. Constraints: The following cannot be used as a key. 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 Range: The value can contain 1 to 40 characters, including letters (case-insensitive), digits, hyphens (-), and underscores (_). Default value: N/A
value_type	Yes	String	Definition: Specifies the value type of the header. Constraints: N/A Range: USER_DEFINED , REFERENCE_HEADER , or SYSTEM_DEFINED Default value: N/A

Parameter	Mandatory	Type	Description
value	Yes	String	Definition: Specifies the value of the header. Constraints: 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 . Range: 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. Default value: N/A

Table 5-631 UpdateRemoveHeadersConfig

Parameter	Mandatory	Type	Description
configs	Yes	Array of UpdateRemoveHeaderConfig objects	Definition: Specifies the headers you want to remove from the request that matches the forwarding rule. Default value: N/A

Table 5-632 UpdateRemoveHeaderConfig

Parameter	Mandatory	Type	Description
key	Yes	String	Definition: Specifies the key of the header you want to remove from the request that matches the forwarding rule. Constraints: The following cannot be used as a key. 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 Range: The value can contain 1 to 40 characters, including letters (case-insensitive), digits, hyphens (-), and underscores (_). Default value: N/A

Table 5-633 UpdateTrafficLimitConfig

Parameter	Mandatory	Type	Description
qps	No	Integer	Definition: Specifies the maximum number of queries per second (QPS). Constraints: N/A Range: 0 to 100000. Unit: count/s. 0 indicates that QPS is not limited. Default value: N/A

Parameter	Mandatory	Type	Description
per_source_ip_qps	No	Integer	Definition: Specifies the maximum number of queries per second (QPS) from a source IP address (single client). Constraints: • This parameter is not available for QUIC listeners. • The value can be 0 or null. • If qps is not set to 0, per_source_ip_qps must be specified a smaller value than qps. Range: 0 to 100000. Unit: count/s. 0 indicates that QPS is not limited. Default value: N/A
burst	No	Integer	Definition: Specifies the allowed burst queries if the number of queries exceeds the value specified for qps. If the number of burst queries exceeds the value specified for burst, 503 Service Unavailable will be returned to the client. Constraints: N/A Range: 0 to 100000. Unit: count/s. Default value: N/A

Table 5-634 CreateCorsConfig

Parameter	Mandatory	Type	Description
allow_origin	No	Array of strings	Definition: 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. Range: N/A Default value: N/A
allow_methods	No	Array of strings	Definition: Specifies the HTTP methods that the specified URLs can use to access cross-origin resources. Constraints: N/A Range: N/A Default value: N/A
allow_headers	No	Array of strings	Definition: Specifies the request headers that can be carried in CORS requests. Constraints: N/A Range: N/A Default value: N/A
expose_headers	No	Array of strings	Definition: Specifies the headers that can be exposed. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
allow_credentials	No	Boolean	Definition: Specifies whether to allow credentials in CORS requests. Constraints: N/A Range: • true: Credentials are allowed. • false: Credentials are not allowed. Default value: N/A
max_age	No	Long	Definition: Specifies the maximum duration a preflight request can be cached, in seconds. Constraints: N/A Range: -1 to 172800 Default value: N/A

Table 5-635 CreateTrafficMirrorConfig

Parameter	Mandatory	Type	Description
target_ids	No	Array of strings	Definition: Specifies the IDs of the backend server groups that traffic is mirrored to. Constraints: N/A Range: N/A Default value: N/A
mirror_request_body_enable	No	Boolean	Specifies whether to include the mirror request body. The default value is true . Constraints: N/A Range: N/A Default value: N/A

Table 5-636 CreateRuleOption

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Definition: Specifies the administrative status of the forwarding rule. Constraints: The value can only be true . Range: N/A Default value: N/A
compare_type	Yes	String	Definition: Specifies how requests are matched with the forwarding rule. Constraints: • 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. Range: • EQUAL_TO: exact match • REGEX: regular expression match • STARTS_WITH: prefix match Default value: N/A

Parameter	Mandatory	Type	Description
key	No	String	Definition: 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. Constraints: N/A Range: N/A Default value: N/A This parameter is unsupported. Please do not use it.

Parameter	Mandatory	Type	Description
value	Yes	String	Definition: Specifies the value of the match item. For example, if a domain name is used for matching, value is the domain name. Constraints: This parameter takes effect only when conditions is left blank. Range: • If type is set to HOST_NAME, the value can contain 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 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. Default value: N/A
project_id	No	String	Definition: Specifies the ID of the project where the forwarding rule is used. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
type	Yes	String	Definition: Specifies the forwarding rule type. Constraints: 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. Range: • HOST_NAME: A domain name will be used for matching. • PATH: A URL will be used for matching. • METHOD: A request method will be used for matching. • HEADER: A request header will be used for matching. • QUERY_STRING: A query string will be used for matching. • SOURCE_IP: A source IP address will be used for matching. • COOKIE: A cookie will be used for matching. Default value: N/A
invert	No	Boolean	Definition: Specifies whether reverse matching is supported. Constraints: N/A 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	Definition: Specifies the conditions contained in a forwarding rule. Constraints: • This parameter takes effect only when enhance_l7policy_enable is set to true. • If conditions is set for a forwarding rule, the values of key and value are ignored. • All keys in the conditions of a rule must be the same, and the values must be unique. Range: N/A Default value: N/A

Table 5-637 CreateRuleCondition

Parameter	Mandatory	Type	Description
key	No	String	Definition: Specifies the key of match item. Constraints: All keys in the conditions list in the same rule must be the same. Range: • 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. Each key 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 allowed. Default value: N/A

Parameter	Mandatory	Type	Description
value	Yes	String	Definition: Specifies the value of the match item. Constraints: • The key of each condition in a forwarding rule must be the same. • The value of each condition in a forwarding rule must be unique. Range: • If type is set to HOST_NAME, key is always an empty string and value indicates the domain name. Each value 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 always an empty string and value indicates the request path, which can contain 1 to 128 characters. If compare_type is set to STARTS_WITH or EQUAL_TO for a forwarding rule, the value must start with a slash (/) and can contain only letters, digits, and special characters: _~';@^-%#&\$. * +?,=!: \\V()[]{}. • 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 128 characters. Asterisks (*) and question marks (?) are

Parameter	Mandatory	Type	Description
			allowed, but spaces and double quotation marks are not allowed. An asterisk can match zero or more characters, and a question mark can match one 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 allowed. Asterisks (*) and question marks (?) are allowed. An asterisk can match zero or more characters, and a question mark can match one character. • If type is set to METHOD, key is always an empty string and 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 always an empty string and 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. Default value: N/A

Response Parameters

Status code: 200

Table 5-638 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
l7policy	L7Policy object	Definition: Specifies the forwarding policy.

Table 5-639 L7Policy

Parameter	Type	Description
action	String	Definition: Specifies the action of the forwarding policy. Range: • 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.
admin_state_up	Boolean	Definition: Specifies the administrative status of the forwarding policy. Range: The value can only be true .
description	String	Definition: Provides supplementary information about the forwarding policy. Range: N/A
id	String	Definition: Specifies the forwarding policy ID. Range: N/A

Parameter	Type	Description
listener_id	String	Definition: Specifies the ID of the listener with which the forwarding policy is associated. Range: N/A
name	String	Definition: Specifies the forwarding policy name. Range: N/A
position	Integer	Definition: Specifies the priority of the forwarding policy. The priority cannot be updated. This parameter is unsupported. Please do not use it.
priority	Integer	Definition: Specifies the priority of the forwarding policy. A smaller value indicates a higher priority. Range: - 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.
project_id	String	Definition: Specifies the ID of the project where the forwarding policy is used. Range: N/A
provisioning_status	String	Definition: Specifies the provisioning status of the forwarding policy. Range: ACTIVE (default): The forwarding policy is provisioned successfully. ERROR: The forwarding policy has the same rule as another forwarding policy added to the same listener.
redirect_pool_id	String	Definition: Specifies the ID of the backend server group to which requests will be forwarded. Range: N/A
redirect_listener_id	String	Definition: Specifies the ID of the listener to which requests are redirected. Range: N/A

Parameter	Type	Description
redirect_url	String	Definition: Specifies the URL to which requests will be forwarded. Range: The value must be in the format of <i>protocol://host:port/path?query</i> . This parameter is unsupported. Please do not use it.
rules	Array of RuleRef objects	Definition: Lists the forwarding rules in the forwarding policy.
redirect_url_config	RedirectUrlConfig object	Definition: Specifies the URL to which requests are forwarded.
redirect_pools_config	Array of RedirectPoolsConfig objects	Definition: Specifies the backend server groups that the requests are forwarded to. This parameter takes effect only when enhance_l7policy_enable is set to true . If this parameter is specified and enhance_l7policy_enable is set to false , an error will be returned.
redirect_pools_sticky_session_config	RedirectPoolsStickySessionConfig object	Definition: 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 group.
redirect_pools_extend_config	RedirectPoolsExtendConfig object	Definition: Specifies the backend server group that requests are forwarded to.
fixed_response_config	FixedResponseConfig object	Definition: Specifies the configuration of the page that will be returned.
created_at	String	Definition: Specifies the creation time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format. Note: This parameter 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	Definition: Specifies the update time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format. Note: This parameter 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	Definition: Specifies the enterprise project ID. Range: N/A

Table 5-640 RuleRef

Parameter	Type	Description
id	String	Definition: Specifies the forwarding rule ID. Range: N/A

Table 5-641 RedirectUrlConfig

Parameter	Type	Description
protocol	String	Definition: Specifies the protocol for redirection. Range: • HTTP • HTTPS • \${protocol}: indicates that the protocol in the request will be used.
host	String	Definition: Specifies the name of the host that requests are redirected to. Range: The value can contain only letters, digits, hyphens (-), and periods (.) and must start with a letter or digit.
port	String	Definition: Specifies the port that requests are redirected to. Range: N/A

Parameter	Type	Description
path	String	Definition: Specifies the path that requests are redirected to. Range: The value can contain only letters, digits, and special characters: <code>_~';@^-%#&\$. *+?,=!: \/()[]{} </code> and must start with a slash (/).
query	String	Definition: Specifies the query string set in the URL for redirection. The following is an example: In the URL https://www.example.com:8080/elb?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 . In the example, `\${query}` indicates type=loadbalancer . Range: The value can contain only letters, digits, and the special characters: <code>!\$&'()*+,-./:;=?@^_` </code> . The letters are case-sensitive. <code>\$1</code> , <code>\$2</code> , <code>\$3</code> , and all the way to <code>\$9</code> match the wildcard asterisk (*) in the requested URL.
status_code	String	Definition: Specifies the status code returned after the requests are redirected. Range: • 301 • 302 • 303 • 307 • 308
insert_headers_config	InsertHeadersConfig object	Definition: Specifies the headers you want to write into the request that matches the forwarding rule.
remove_headers_config	RemoveHeadersConfig object	Definition: Specifies the headers you want to remove from the request that matches the forwarding rule.

Table 5-642 RedirectPoolsConfig

Parameter	Type	Description
pool_id	String	Definition: Specifies the backend server group ID. Range: N/A
weight	Integer	Definition: Specifies the weight of the backend server group. Requests are routed to backend server groups based on their weights. The larger the weight is, the higher proportion of requests the backend server group receives. If the weight is set to 0, the backend server group will not accept new requests. Range: 0 to 100

Table 5-643 RedirectPoolsStickySessionConfig

Parameter	Type	Description
enable	Boolean	Definition: Specifies whether to enable sticky session for backend server groups configured in a forwarding policy. Default value: false , indicating that sticky session is disabled.
timeout	Integer	Definition: Specifies the stickiness duration, in minutes. Range: 1 to 1440

Table 5-644 RedirectPoolsExtendConfig

Parameter	Type	Description
rewrite_url_enable	Boolean	Definition: Specifies whether to set rewrite_url_enable to true . Range: The value can be true (enable this option) or false (disable this option).
rewrite_url_config	RewriteUrlConfig object	Definition: Specifies the URL for the backend server group that requests are forwarded to.

Parameter	Type	Description
insert_headers_config	InsertHeadersConfig object	Definition: Specifies the headers you want to write into the request that matches the forwarding rule.
remove_headers_config	RemoveHeadersConfig object	Definition: Specifies the headers you want to remove from the request that matches the forwarding rule.
traffic_limit_config	TrafficLimitConfig object	Definition: Specifies how requests are limited.
cors_config	CorsConfig object	Definition: Specifies the CORS configurations.
traffic_mirror_config	TrafficMirrorConfig object	Definition: Specifies the traffic mirroring configuration.

Table 5-645 RewriteUrlConfig

Parameter	Type	Description
host	String	Definition: Specifies the domain name of the host that requests are redirected to. Range: The value can contain letters, digits, hyphens (-), and periods (.), and must start with a letter or digit.
path	String	Definition: Specifies the path that requests are redirected to. \$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 \$# . Range: The value must start with a slash (/) and can contain only letters, digits, and special characters: _~';@^-%#&\$.+?,=!: /()

Parameter	Type	Description
query	String	Definition: Specifies the query string set in the URL for redirection. \$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 \$# . Range: The value can contain only letters, digits, and the special characters: !\$&'()+,-./:;=?@^_`. The letters are case-sensitive.

Table 5-646 CorsConfig

Parameter	Type	Description
allow_origin	Array of strings	Definition: 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	Definition: Specifies the HTTP methods that the specified URLs can use to access cross-origin resources. Range: N/A
allow_headers	Array of strings	Definition: Specifies the request headers that can be carried in CORS requests. Range: N/A

Parameter	Type	Description
expose_headers	Array of strings	Definition: Specifies the headers that can be exposed. Range: N/A
allow_credentials	Boolean	Definition: Specifies whether to allow credentials in CORS requests. Range: • true: Credentials are allowed. • false: Credentials are not allowed.
max_age	Long	Definition: Specifies the maximum duration a preflight request can be cached, in seconds. Range: -1 to 172800

Table 5-647 TrafficMirrorConfig

Parameter	Type	Description
target_ids	Array of strings	Definition: Specifies the IDs of the backend server groups that traffic is mirrored to. Range: N/A
mirror_request_body_enable	Boolean	Specifies whether to include the mirror request body. The default value is true . Range: N/A

Table 5-648 FixedResponseConfig

Parameter	Type	Description
status_code	String	Definition: Specifies the HTTP status code. Range: 200-299, 400-499, 500-599
content_type	String	Definition: Specifies the format of the returned body. Range: • text/plain • text/css • text/html • application/javascript • application/json

Parameter	Type	Description
message_body	String	Definition: Specifies the content of the response message body. Range: N/A
insert_headers_config	InsertHeadersConfig object	Definition: Specifies the headers you want to write into the request that matches the forwarding rule.
remove_headers_config	RemoveHeadersConfig object	Definition: Specifies the headers you want to remove from the request that matches the forwarding rule.
traffic_limit_config	TrafficLimitConfig object	Definition: Specifies how requests are limited.

Table 5-649 InsertHeadersConfig

Parameter	Type	Description
configs	Array of InsertHeaderConfig objects	Definition: Specifies the headers you want to write into the request that matches the forwarding rule. Constraints: N/A

Table 5-650 InsertHeaderConfig

Parameter	Type	Description
key	String	Definition: Specifies the key of the header you want to write into the request that matches the forwarding rule. Range: The value can contain 1 to 40 characters, including letters (case-insensitive), digits, hyphens (-), and underscores (_).
value_type	String	Definition: Specifies the value type of the header. Range: USER_DEFINED , REFERENCE_HEADER , or SYSTEM_DEFINED

Parameter	Type	Description
value	String	Definition: Specifies the value of the header. Range: 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 5-651 RemoveHeadersConfig

Parameter	Type	Description
configs	Array of RemoveHeaderConfig objects	Definition: Specifies the headers you want to remove from the request that matches the forwarding rule. Constraints: N/A

Table 5-652 RemoveHeaderConfig

Parameter	Type	Description
key	String	Definition: Specifies the key of the header you want to remove from the request that matches the forwarding rule. Range: The value can contain 1 to 40 characters, including letters (case-insensitive), digits, hyphens (-), and underscores (_).

Table 5-653 TrafficLimitConfig

Parameter	Type	Description
qps	Integer	Definition: Specifies the maximum number of queries per second (QPS). Range: 0 to 100000. Unit: count/s. 0 indicates that QPS is not limited.

Parameter	Type	Description
per_source_ip_qps	Integer	Definition: Specifies the maximum number of queries per second (QPS) from a source IP address (single client). Range: 0 to 100000. Unit: count/s. 0 indicates that QPS is not limited.
burst	Integer	Definition: Specifies the allowed burst queries if the number of queries exceeds the value specified for qps . If the number of burst queries exceeds the value specified for burst , 503 Service Unavailable will be returned to the client. Range: 0 to 100000. Unit: count/s.

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 5-654 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
l7policy_id	Yes	String	Definition: Specifies the forwarding policy ID. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-655 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 204

Successful request.

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 huaweicloudskelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskelb.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 5-656 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-657 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-658 Request body parameters

Parameter	Mandatory	Type	Description
l7policies	No	Array of BatchUpdatePriorityRequestBody objects	Definition: Request parameters for batch modifying forwarding policy priorities Constraints: N/A

Table 5-659 BatchUpdatePriorityRequestBody

Parameter	Mandatory	Type	Description
id	Yes	String	Definition: Specifies the ID of the forwarding policy to be updated. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
priority	Yes	Integer	Definition: Specifies the priority of the forwarding policy. A smaller value indicates a higher priority. Constraints: • The priority 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 set to false, 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 unsupported for shared load balancers. Range: • If action is set to REDIRECT_TO_LISTENER, the priority ranges from 0 to 10,000.

Parameter	Mandatory	Type	Description
			• If action is set to other values, the priority ranges from 1 to 10,000. Default value: • 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 there is no forwarding policy, the priority of a new forwarding policy will be 1 by default. – If the priority of an existing forwarding policy is the maximum value (10,000), the forwarding policy will fail to be created because the maximum value will be exceeded. In this case, specify a value or adjust the priorities of existing forwarding policies.

Response Parameters

Status code: 202

Table 5-660 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Constraints: N/A

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

The forwarding rule cannot be created when **action** is set to **REDIRECT_TO_LISTENER**.

Calling Method

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

URI

POST /v3/{project_id}/elb/l7policies/{l7policy_id}/rules

Table 5-661 Path Parameters

Parameter	Mandatory	Type	Description
l7policy_id	Yes	String	Definition: Specifies the forwarding policy ID. Constraints: N/A Range: N/A Default value: N/A
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-662 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-663 Request body parameters

Parameter	Mandatory	Type	Description
rule	Yes	CreateRuleOption object	Definition: Specifies the forwarding rule. Constraints: N/A

Table 5-664 CreateRuleOption

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Definition: Specifies the administrative status of the forwarding rule. Constraints: The value can only be true . Range: N/A Default value: N/A
compare_type	Yes	String	Definition: Specifies how requests are matched with the forwarding rule. Constraints: • 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. Range: • EQUAL_TO: exact match • REGEX: regular expression match • STARTS_WITH: prefix match Default value: N/A

Parameter	Mandatory	Type	Description
key	No	String	Definition: 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. Constraints: N/A Range: N/A Default value: N/A This parameter is unsupported. Please do not use it.

Parameter	Mandatory	Type	Description
value	Yes	String	Definition: Specifies the value of the match item. For example, if a domain name is used for matching, value is the domain name. Constraints: This parameter takes effect only when conditions is left blank. Range: • If type is set to HOST_NAME, the value can contain 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 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. Default value: N/A
project_id	No	String	Definition: Specifies the ID of the project where the forwarding rule is used. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
type	Yes	String	Definition: Specifies the forwarding rule type. Constraints: 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. Range: • HOST_NAME: A domain name will be used for matching. • PATH: A URL will be used for matching. • METHOD: A request method will be used for matching. • HEADER: A request header will be used for matching. • QUERY_STRING: A query string will be used for matching. • SOURCE_IP: A source IP address will be used for matching. • COOKIE: A cookie will be used for matching. Default value: N/A
invert	No	Boolean	Definition: Specifies whether reverse matching is supported. Constraints: N/A 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	Definition: Specifies the conditions contained in a forwarding rule. Constraints: • This parameter takes effect only when enhance_l7policy_enable is set to true. • If conditions is set for a forwarding rule, the values of key and value are ignored. • All keys in the conditions of a rule must be the same, and the values must be unique. Range: N/A Default value: N/A

Table 5-665 CreateRuleCondition

Parameter	Mandatory	Type	Description
key	No	String	Definition: Specifies the key of match item. Constraints: All keys in the conditions list in the same rule must be the same. Range: • 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. Each key 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 allowed. Default value: N/A

Parameter	Mandatory	Type	Description
value	Yes	String	Definition: Specifies the value of the match item. Constraints: • The key of each condition in a forwarding rule must be the same. • The value of each condition in a forwarding rule must be unique. Range: • If type is set to HOST_NAME, key is always an empty string and value indicates the domain name. Each value 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 always an empty string and value indicates the request path, which can contain 1 to 128 characters. If compare_type is set to STARTS_WITH or EQUAL_TO for a forwarding rule, the value must start with a slash (/) and can contain only letters, digits, and special characters: _~';@^-%#&\$.*+? ,=!: \\V()[]{}. • 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 128 characters. Asterisks (*) and question marks (?) are

Parameter	Mandatory	Type	Description
			allowed, but spaces and double quotation marks are not allowed. An asterisk can match zero or more characters, and a question mark can match one 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 allowed. Asterisks (*) and question marks (?) are allowed. An asterisk can match zero or more characters, and a question mark can match one character. • If type is set to METHOD, key is always an empty string and 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 always an empty string and 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. Default value: N/A

Response Parameters

Status code: 201

Table 5-666 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
rule	L7Rule object	Definition: Specifies the forwarding rule.

Table 5-667 L7Rule

Parameter	Type	Description
admin_state_up	Boolean	Definition: Specifies the administrative status of the forwarding rule. Range: The value can only be true . This parameter is unsupported. Please do not use it.
compare_type	String	Definition: Specifies how requests are matched with the forwarding rule. Range: 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	Definition: Specifies the key of the match content. Range: N/A
project_id	String	Definition: Specifies the ID of the project where the forwarding rule is used. Range: N/A

Parameter	Type	Description
type	String	Definition: Specifies the forwarding rule type. Range: • HOST_NAME: A domain name will be used for matching. • PATH: A URL will be used for matching. • METHOD: A request method will be used for matching. • HEADER: A request header will be used for matching. • QUERY_STRING: A query string will be used for matching. • SOURCE_IP: A source IP address will be used for matching. • COOKIE: A cookie will be used for matching.
value	String	Definition: Specifies the value of the match item. Range: • If type is set to HOST_NAME, the value can contain 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 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: <code>_~'!;@^-%#&\$. *+?,= :\ /() []{} </code> • 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	Type	Description
provisioning_status	String	Definition: Specifies the provisioning status of the forwarding rule. This parameter is invalid. The default value is ACTIVE . Range: ACTIVE , PENDING_CREATE , or ERROR .
invert	Boolean	Definition: Specifies whether reverse matching is supported. Range: N/A
id	String	Definition: Specifies the forwarding rule ID. Range: N/A
conditions	Array of RuleCondition objects	Definition: Specifies the conditions contained in a forwarding rule. Range: N/A
created_at	String	Definition: Specifies the creation time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format. Note: This parameter 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	Definition: Specifies the update time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format. Note: This parameter will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.

Table 5-668 RuleCondition

Parameter	Type	Description
key	String	Definition: Specifies the key of match item. Constraints: All keys in the conditions list in the same rule must be the same. Range: • 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. Each key 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 allowed. Default value: N/A

Parameter	Type	Description
value	String	Definition: Specifies the value of the match item. Constraints: The value of each condition in a forwarding rule must be unique. Range: • If type is set to HOST_NAME, key is always an empty string and value indicates the domain name. Each value 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 always an empty string and value indicates the request path, which can contain 1 to 128 characters. If compare_type is set to STARTS_WITH or EQUAL_TO for a 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 request 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 one 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 allowed. Asterisks (*) and question marks (?) are allowed. An asterisk can match zero or more characters, and a question mark can match one character. • If type is set to METHOD, key is always an empty string and 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 always an empty string and 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. Default value: N/A

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

Successful request.

```
{
  "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.ElClientBuilder().
            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	Successful request.

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 5-669 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
l7policy_id	Yes	String	Definition: Specifies the forwarding policy ID. Constraints: N/A Range: N/A Default value: N/A

Table 5-670 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Definition: Specifies the number of records returned on each page. Constraints: N/A Range: 0 to 2000 Default value: 2000

Parameter	Mandatory	Type	Description
marker	No	String	Definition: Specifies the ID of the last record on the previous page. Constraints: • This parameter must be used together with limit. • If the parameter is not specified, only resources on the first page are queried. • This parameter cannot be left blank or set to an invalid ID. Range: N/A Default value: N/A
page_reverse	No	Boolean	Definition: Specifies whether to use reverse query. Constraints: • This parameter must be used together with limit. • If page_reverse is set to true and you want to query the resources on the previous page, set the value of marker to the value of previous_marker. Range: • true: Query resources on the previous page. • false: Query resources on the next page. Default value: false
id	No	Array of strings	Definition: Specifies the forwarding rule ID. Multiple IDs can be used for query in the format of <i>id=xxx&id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
compare_type	No	Array of strings	Definition: Specifies how requests are matched. Multiple values can be used for query in the format of <i>compare_type=xxx&compare_type=xxx</i> . Range: • EQUAL_TO: exact match. • REGEX: regular expression match • STARTS_WITH: prefix match Default value: N/A
provisioning_status	No	Array of strings	Definition: Specifies the provisioning status of the forwarding rule. Multiple provisioning statuses can be used for query in the format of <i>provisioning_status=xxx&provisioning_status=xxx</i> . Constraints: N/A Range: The value can only be ACTIVE , indicating that the forwarding rule is provisioned successfully. Default value: N/A
invert	No	Boolean	Definition: Specifies whether reverse matching is supported. Constraints: N/A Range: false Default value: N/A
admin_state_up	No	Boolean	Definition: Specifies the administrative status of the forwarding rule. This parameter is unsupported. Please do not use it. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
value	No	Array of strings	Definition: Specifies the value of the match content. Multiple values can be used for query in the format of <i>value=xxx&value=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
key	No	Array of strings	Definition: Specifies the key of the match content that is used to identify the forwarding rule. Multiple keys can be used for query in the format of <i>key=xxx&key=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
type	No	Array of strings	Definition: Specifies the match type. The value can be HOST_NAME or PATH . Multiple types can be used for query in the format of <i>type=xxx&type=xxx</i> . Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
enterprise_project_id	No	Array of strings	Definition: Specifies the ID of the enterprise project. Multiple values can be used for query in the format of: <i>enterprise_project_id=xxx&enterprise_project_id=xxx.</i> Constraints: • 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. Range: N/A Default value: N/A

Request Parameters

Table 5-671 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-672 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
page_info	PageInfo object	Definition: Specifies the pagination information.
rules	Array of L7Rule objects	Definition: Lists the forwarding rules.

Table 5-673 PageInfo

Parameter	Type	Description
previous_marker	String	Definition: Specifies the ID of the first record in the pagination query result. If page_reverse is set to true , this parameter is used together to query resources on the previous page. Range: N/A
next_marker	String	Definition: Specifies the ID of the last record in the pagination query result. It is usually used to query resources on the next page. Range: N/A
current_count	Integer	Definition: Specifies the number of records returned on the current page. Range: N/A

Table 5-674 L7Rule

Parameter	Type	Description
admin_state_up	Boolean	Definition: Specifies the administrative status of the forwarding rule. Range: The value can only be true . This parameter is unsupported. Please do not use it.
compare_type	String	Definition: Specifies how requests are matched with the forwarding rule. Range: 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	Definition: Specifies the key of the match content. Range: N/A
project_id	String	Definition: Specifies the ID of the project where the forwarding rule is used. Range: N/A
type	String	Definition: Specifies the forwarding rule type. Range: • HOST_NAME: A domain name will be used for matching. • PATH: A URL will be used for matching. • METHOD: A request method will be used for matching. • HEADER: A request header will be used for matching. • QUERY_STRING: A query string will be used for matching. • SOURCE_IP: A source IP address will be used for matching. • COOKIE: A cookie will be used for matching.

Parameter	Type	Description
value	String	Definition: Specifies the value of the match item. Range: - If type is set to HOST_NAME, the value can contain 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 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.
provisioning_status	String	Definition: Specifies the provisioning status of the forwarding rule. This parameter is invalid. The default value is ACTIVE . Range: ACTIVE , PENDING_CREATE , or ERROR .
invert	Boolean	Definition: Specifies whether reverse matching is supported. Range: N/A
id	String	Definition: Specifies the forwarding rule ID. Range: N/A
conditions	Array of RuleCondition objects	Definition: Specifies the conditions contained in a forwarding rule. Range: N/A

Parameter	Type	Description
created_at	String	Definition: Specifies the creation time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format. Note: This parameter 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	Definition: Specifies the update time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format. Note: This parameter will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.

Table 5-675 RuleCondition

Parameter	Type	Description
key	String	Definition: Specifies the key of match item. Constraints: All keys in the conditions list in the same rule must be the same. Range: • 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. Each key 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 allowed. Default value: N/A

Parameter	Type	Description
value	String	Definition: Specifies the value of the match item. Constraints: The value of each condition in a forwarding rule must be unique. Range: • If type is set to HOST_NAME, key is always an empty string and value indicates the domain name. Each value 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 always an empty string and value indicates the request path, which can contain 1 to 128 characters. If compare_type is set to STARTS_WITH or EQUAL_TO for a 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 request 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 one 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 allowed. Asterisks (*) and question marks (?) are allowed. An asterisk can match zero or more characters, and a question mark can match one character. • If type is set to METHOD, key is always an empty string and 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 always an empty string and 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. Default value: N/A

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.getErrMsg());
        }
    }
}
```

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 5-676 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Parameter	Mandatory	Type	Description
l7policy_id	Yes	String	Definition: Specifies the forwarding policy. Constraints: N/A Range: N/A Default value: N/A
l7rule_id	Yes	String	Definition: Specifies the forwarding rule. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-677 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-678 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
rule	L7Rule object	Definition: Specifies the forwarding rule.

Table 5-679 L7Rule

Parameter	Type	Description
admin_state_up	Boolean	Definition: Specifies the administrative status of the forwarding rule. Range: The value can only be true . This parameter is unsupported. Please do not use it.
compare_type	String	Definition: Specifies how requests are matched with the forwarding rule. Range: 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	Definition: Specifies the key of the match content. Range: N/A
project_id	String	Definition: Specifies the ID of the project where the forwarding rule is used. Range: N/A
type	String	Definition: Specifies the forwarding rule type. Range: • HOST_NAME: A domain name will be used for matching. • PATH: A URL will be used for matching. • METHOD: A request method will be used for matching. • HEADER: A request header will be used for matching. • QUERY_STRING: A query string will be used for matching. • SOURCE_IP: A source IP address will be used for matching. • COOKIE: A cookie will be used for matching.

Parameter	Type	Description
value	String	Definition: Specifies the value of the match item. Range: - If type is set to HOST_NAME, the value can contain 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 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: <code>_~';@^-%#&\$. *+?,=!: \/()</code> <code>[]{}.</code> - 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.
provisioning_status	String	Definition: Specifies the provisioning status of the forwarding rule. This parameter is invalid. The default value is ACTIVE . Range: ACTIVE , PENDING_CREATE , or ERROR .
invert	Boolean	Definition: Specifies whether reverse matching is supported. Range: N/A
id	String	Definition: Specifies the forwarding rule ID. Range: N/A
conditions	Array of RuleCondition objects	Definition: Specifies the conditions contained in a forwarding rule. Range: N/A

Parameter	Type	Description
created_at	String	Definition: Specifies the creation time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format. Note: This parameter 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	Definition: Specifies the update time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format. Note: This parameter will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.

Table 5-680 RuleCondition

Parameter	Type	Description
key	String	Definition: Specifies the key of match item. Constraints: All keys in the conditions list in the same rule must be the same. Range: • 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. Each key 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 allowed. Default value: N/A

Parameter	Type	Description
value	String	Definition: Specifies the value of the match item. Constraints: The value of each condition in a forwarding rule must be unique. Range: • If type is set to HOST_NAME, key is always an empty string and value indicates the domain name. Each value 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 always an empty string and value indicates the request path, which can contain 1 to 128 characters. If compare_type is set to STARTS_WITH or EQUAL_TO for a 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 request 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 one 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 allowed. Asterisks (*) and question marks (?) are allowed. An asterisk can match zero or more characters, and a question mark can match one character. • If type is set to METHOD, key is always an empty string and 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 always an empty string and 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. Default value: N/A

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

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from 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 5-681 Path Parameters

Parameter	Mandatory	Type	Description
l7policy_id	Yes	String	Definition: Specifies the forwarding policy ID. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
l7rule_id	Yes	String	Definition: Specifies the forwarding rule ID. Constraints: N/A Range: N/A Default value: N/A
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-682 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-683 Request body parameters

Parameter	Mandatory	Type	Description
rule	Yes	UpdateL7RuleOption object	Definition: Specifies the forwarding rule. Constraints: N/A

Table 5-684 UpdateL7RuleOption

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Definition: Specifies the administrative status of the forwarding rule. Constraints: The value can only be true . Range: N/A Default value: N/A
compare_type	No	String	Definition: Specifies how requests are matched with the forwarding rule. Constraints: • 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. Range: • EQUAL_TO: exact match • REGEX: regular expression match • STARTS_WITH: prefix match Default value: N/A

Parameter	Mandatory	Type	Description
invert	No	Boolean	Definition: Specifies whether reverse matching is supported. Constraints: N/A Range: true or false Default value: false This parameter is unsupported. Please do not use it.
key	No	String	Definition: 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. Constraints: N/A Range: N/A Default value: N/A This parameter is unsupported. Please do not use it.

Parameter	Mandatory	Type	Description
value	No	String	Definition: Specifies the value of the match item. For example, if a domain name is used for matching, value is the domain name. Constraints: This parameter takes effect only when conditions is left blank. Range: • If type is set to HOST_NAME, the value can contain 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 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: <code>_~' ;@^-%#&\$. * + ?, = ! : \ / () [] { }</code> • 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. Default value: N/A

Parameter	Mandatory	Type	Description
conditions	No	Array of UpdateRuleCondition objects	Definition: Specifies the conditions contained in a forwarding rule. Constraints: • This parameter takes effect only when enhance_l7policy_enable is set to true. • If conditions is set for a forwarding rule, the values of key and value are ignored. • All keys in the conditions of a rule must be the same, and the values must be unique. Range: N/A Default value: N/A

Table 5-685 UpdateRuleCondition

Parameter	Mandatory	Type	Description
key	No	String	Definition: Specifies the key of match item. Constraints: All keys in the conditions list in the same rule must be the same. Range: • 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. Each key 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 allowed. Default value: N/A

Parameter	Mandatory	Type	Description
value	No	String	Definition: Specifies the value of the match item. Constraints: • The key of each condition in a forwarding rule must be the same. • The value of each condition in a forwarding rule must be unique. Range: • If type is set to HOST_NAME, key is always an empty string and value indicates the domain name. Each value 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 always an empty string and value indicates the request path, which can contain 1 to 128 characters. If compare_type is set to STARTS_WITH or EQUAL_TO for a forwarding rule, the value must start with a slash (/) and can contain only letters, digits, and special characters: _~';@^-%#&\$. * +?,=!: \\V()[]{}. • 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 128 characters. Asterisks (*) and question marks (?) are

Parameter	Mandatory	Type	Description
			allowed, but spaces and double quotation marks are not allowed. An asterisk can match zero or more characters, and a question mark can match one 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 allowed. Asterisks (*) and question marks (?) are allowed. An asterisk can match zero or more characters, and a question mark can match one character. • If type is set to METHOD, key is always an empty string and 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 always an empty string and 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. Default value: N/A

Response Parameters

Status code: 200

Table 5-686 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
rule	L7Rule object	Definition: Specifies the forwarding rule.

Table 5-687 L7Rule

Parameter	Type	Description
admin_state_up	Boolean	Definition: Specifies the administrative status of the forwarding rule. Range: The value can only be true . This parameter is unsupported. Please do not use it.
compare_type	String	Definition: Specifies how requests are matched with the forwarding rule. Range: 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	Definition: Specifies the key of the match content. Range: N/A
project_id	String	Definition: Specifies the ID of the project where the forwarding rule is used. Range: N/A

Parameter	Type	Description
type	String	Definition: Specifies the forwarding rule type. Range: • HOST_NAME: A domain name will be used for matching. • PATH: A URL will be used for matching. • METHOD: A request method will be used for matching. • HEADER: A request header will be used for matching. • QUERY_STRING: A query string will be used for matching. • SOURCE_IP: A source IP address will be used for matching. • COOKIE: A cookie will be used for matching.
value	String	Definition: Specifies the value of the match item. Range: • If type is set to HOST_NAME, the value can contain 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 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: <code>_~'!;@^-%#&\$. *+?,= :\ /() []{} </code> • 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	Type	Description
provisioning_status	String	Definition: Specifies the provisioning status of the forwarding rule. This parameter is invalid. The default value is ACTIVE . Range: ACTIVE , PENDING_CREATE , or ERROR .
invert	Boolean	Definition: Specifies whether reverse matching is supported. Range: N/A
id	String	Definition: Specifies the forwarding rule ID. Range: N/A
conditions	Array of RuleCondition objects	Definition: Specifies the conditions contained in a forwarding rule. Range: N/A
created_at	String	Definition: Specifies the creation time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format. Note: This parameter 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	Definition: Specifies the update time. Range: The value must be a UTC time in the <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> format. Note: This parameter will not be returned for resources associated with existing dedicated load balancers and for resources associated with existing and new shared load balancers.

Table 5-688 RuleCondition

Parameter	Type	Description
key	String	Definition: Specifies the key of match item. Constraints: All keys in the conditions list in the same rule must be the same. Range: • 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. Each key 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 allowed. Default value: N/A

Parameter	Type	Description
value	String	Definition: Specifies the value of the match item. Constraints: The value of each condition in a forwarding rule must be unique. Range: • If type is set to HOST_NAME, key is always an empty string and value indicates the domain name. Each value 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 always an empty string and value indicates the request path, which can contain 1 to 128 characters. If compare_type is set to STARTS_WITH or EQUAL_TO for a 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 request 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 one 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 allowed. Asterisks (*) and question marks (?) are allowed. An asterisk can match zero or more characters, and a question mark can match one character. • If type is set to METHOD, key is always an empty string and 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 always an empty string and 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. Default value: N/A

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.ElClientBuilder().
        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 5-689 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
l7policy_id	Yes	String	Definition: Specifies the forwarding policy ID. Constraints: N/A Range: N/A Default value: N/A
l7rule_id	Yes	String	Definition: Specifies the forwarding rule ID. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-690 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 204

Successful request.

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

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from 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 5-691 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-692 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-693 Request body parameters

Parameter	Mandatory	Type	Description
pool	Yes	CreateMasterSlavePoolOption object	Definition: Specifies the request body for creating an active/standby backend server group. Constraints: N/A

Table 5-694 CreateMasterSlavePoolOption

Parameter	Mandatory	Type	Description
description	No	String	Definition: Specifies the supplementary information about the backend server group. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
lb_algorithm	Yes	String	Definition: Specifies the load balancing algorithm used by the load balancer to route requests to backend servers in the associated backend server group. Constraints: N/A Range: • ROUND_ROBIN: weighted round robin • LEAST_CONNECTIONS: weighted least connections • SOURCE_IP: source IP hash • QUIC_CID: connection ID Default value: N/A
loadbalancer_id	No	String	Definition: Specifies the ID of the load balancer associated with the backend server group. Constraints: Specify at least one of listener_id , loadbalancer_id , or type . Range: N/A Default value: N/A
listener_id	No	String	Definition: Specifies the ID of the listener associated with the backend server group. Constraints: Specify at least one of listener_id , loadbalancer_id , or type . Range: N/A Default value: N/A
name	No	String	Definition: Specifies the backend server group name. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
project_id	No	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A NOTE This parameter is invalid. The project ID in the URL is used.
protocol	Yes	String	Definition: Specifies the protocol used by the backend server group to receive requests. Constraints: • 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 TLS, the protocol of the backend server group can be TLS or TCP. If protocol of the backend server group is TCP, ip_version must be set to v4. Range: The value can be TCP , UDP , QUIC , or TLS . Default value: N/A
session_persistence	No	CreatePoolSessionPersistenceOption object	Definition: Specifies the sticky session. Constraints: Slow start and sticky session cannot be enabled at the same time. If both are enabled, sticky session will be invalid.

Parameter	Mandatory	Type	Description
vpc_id	No	String	Definition: Specifies the ID of the VPC where the backend server group works. Constraints: • 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. Range: N/A Default value: N/A
type	Yes	String	Definition: Specifies the type of the backend server group. Constraints: N/A Range: • 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. Default value: N/A

Parameter	Mandatory	Type	Description
ip_version	No	String	Definition: Specifies the IP address version supported by the backend server group. Constraints: N/A 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. Default value: N/A
members	Yes	Array of CreateMasterSlaveMemberOption objects	Definition: Specifies the backend server of the active/standby server group. Constraints: Only two backend servers can be added, one serving as the active server and the other as the standby server.
healthmonitor	Yes	CreateMasterSlaveHealthMonitorOption object	Definition: Specifies the health check for active/standby backend server group. Health check is enabled by default and cannot be disabled. Constraints: N/A

Parameter	Mandatory	Type	Description
any_port_enable	No	Boolean	Definition: 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 . Constraints: This option is available only for TCP, UDP, and QUIC backend server groups. Range: false (disable this option) or true (enable this option). Constraints: N/A
connection_drain	No	ConnectionDrain object	Definition: Specifies the configurations of deregistration delay. 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. Constraints: This parameter is only available for TCP, UDP, and QUIC backend server groups and TCP and UDP listeners.
quic_cid_hash_strategy	No	QuicCidHashStrategy object	Definition: Specifies multi-path forwarding configuration based on destination connection IDs. Constraints: N/A

Table 5-695 CreatePoolSessionPersistenceOption

Parameter	Mandatory	Type	Description
cookie_name	No	String	Definition: Specifies the cookie name. Constraints: This parameter takes effect only when type is set to APP_COOKIE. Otherwise, an error will be returned. Range: The value can contain a maximum of 1,024 characters. Default value: N/A
type	Yes	String	Definition: Specifies the sticky session type. Constraints: - 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, only HTTP_COOKIE and APP_COOKIE take effect. - If the backend server group's protocol is QUIC, session_persistence must be set to true and type set to SOURCE_IP. Range: SOURCE_IP , HTTP_COOKIE , or APP_COOKIE . Default value: N/A

Parameter	Mandatory	Type	Description
persistence_timeout	No	Integer	Definition: Specifies the stickiness duration, in minutes. Constraints: This parameter will not take effect when type is set to APP_COOKIE . Range: • 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. Default value: N/A

Table 5-696 CreateMasterSlaveMemberOption

Parameter	Mandatory	Type	Description
address	Yes	String	Definition: Specifies the IP address bound to the backend server. Constraints: • If subnet_cidr_id is left blank, IP as backend servers will be added. In this case, the IP address must be an IPv4 address. • If subnet_cidr_id is not left blank, ECSs will be added as backend servers. It must be in the subnet specified by subnet_cidr_id. Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Definition: Specifies the administrative status of the backend server. Constraints: Although this parameter can be used in the APIs for creating and updating backend servers, its actual value depends on whether ECSs exist. Range: If ECSs exist, the value is true . Otherwise, the value is false . Default value: N/A
name	No	String	Definition: Specifies the backend server name. Constraints: N/A Range: N/A Default value: N/A
protocol_port	No	Integer	Definition: Specifies the port used by the backend server to receive requests. Constraints: N/A Range: N/A Default value: N/A 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	Definition: Specifies the ID of the IPv4 or IPv6 subnet where the backend server resides. Constraints: • 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, indicating that an IP as backend server will be added. 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. Range: N/A Default value: N/A
role	Yes	String	Definition: Specifies the type of the backend server. Constraints: N/A Range: • master: active backend server • slave: standby backend server Default value: N/A

Table 5-697 CreateMasterSlaveHealthMonitorOption

Parameter	Mandatory	Type	Description
delay	Yes	Integer	Definition: Specifies the interval between health checks, in seconds. Constraints: N/A Range: 1 to 50 Default value: N/A

Parameter	Mandatory	Type	Description
domain_name	No	String	Definition: Specifies the domain name that HTTP requests are sent to during the health check. Constraints: This parameter is available only when type is set to HTTP or HTTPS . Range: The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter. Default value: null , indicating that the virtual IP address of the load balancer is used as the destination address of HTTP requests
expected_codes	No	String	Definition: Specifies the expected HTTP status code. Constraints: This parameter will take effect only when type is set to HTTP , HTTPS or GRPC . Range: • 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 Default value: If type is set to GRPC , the default value is 0. If type is set to other values, the default value is 200 .
http_method	No	String	Definition: Specifies the HTTP method. Constraints: This parameter is available when type is set to HTTP or HTTPS . Range: GET , HEAD , or POST Default value: GET

Parameter	Mandatory	Type	Description
max_retries	Yes	Integer	Definition: Specifies the number of consecutive health checks when the health check result of a backend server changes from OFFLINE to ONLINE . Constraints: N/A Range: 1 to 10 Default value: N/A
max_retries_down	No	Integer	Definition: Specifies the number of consecutive health checks when the health check result of a backend server changes from ONLINE to OFFLINE . Constraints: N/A Range: 1 to 10 Default value: N/A
monitor_port	No	Integer	Specifies the port used for the health check. Constraints: N/A Range: 1 to 65535 Default value: null, indicating the port of a backend server will be used by default.
name	No	String	Definition: Specifies the health check name. Constraints: N/A Range: N/A Default value: N/A
timeout	Yes	Integer	Definition: 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 . Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
type	Yes	String	Definition: Specifies the health check protocol. Constraints: • 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. Range: The value can be TCP, UDP_CONNECT, HTTP, or HTTPS. Default value: N/A
url_path	No	String	Definition: Specifies the HTTP request path for the health check. The value must start with a slash (/). Constraints: This parameter is available only when type is set to HTTP or HTTPS. Range: The value can contain letters, digits, hyphens (-), slashes (/), periods (.), percentage signs (%), question marks (?), pound signs (#), ampersand signs (&), and the extended character set: <code>_~!()*[]@\$^',+.</code> Default value: /

Table 5-698 ConnectionDrain

Parameter	Mandatory	Type	Description
enable	No	Boolean	Definition: Specifies whether to enable connection_drain . Constraints: N/A Range: The value can be true (enable this option) or false (disable this option). Default value: N/A
timeout	No	Integer	Definition: Specifies the deregistration delay timeout, in seconds. Constraints: N/A Range: 10 to 4000, in seconds. Constraints: N/A

Table 5-699 QuicCidHashStrategy

Parameter	Mandatory	Type	Description
len	Yes	Integer	Definition: Specifies the length of the hash factor in the connection ID. Constraints: This parameter is valid only when the load balancing algorithm is QUIC_CID . Range: 1 to 20 Default value: 3
offset	Yes	Integer	Definition: Specifies the start position in the connection ID as the hash factor. Constraints: This parameter is valid only when the load balancing algorithm is QUIC_CID . Range: 0 to 19 Default value: 1

Response Parameters

Status code: 201

Table 5-700 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
pool	MasterSlavePool object	Definition: Specifies the backend server group.

Table 5-701 MasterSlavePool

Parameter	Type	Description
description	String	Definition: Specifies the supplementary information about the backend server group. Range: N/A
id	String	Definition: Specifies the ID of the backend server group. Range: N/A
lb_algorithm	String	Definition: Specifies the load balancing algorithm used by the load balancer to route requests to backend servers in the associated backend server group. Range: • ROUND_ROBIN: weighted round robin • LEAST_CONNECTIONS: weighted least connections • SOURCE_IP: source IP hash • QUIC_CID: connection ID
listeners	Array of ListenerRef objects	Definition: Specifies the IDs of the listeners with which the backend server group is associated.
loadbalancers	Array of LoadBalancerRef objects	Definition: Specifies the IDs of the load balancers with which the active/standby backend server group is associated.
members	Array of MasterSlaveMember objects	Definition: Specifies the backend servers in the backend server group.

Parameter	Type	Description
name	String	Definition: Specifies the backend server group name. Range: N/A
project_id	String	Definition: Specifies the ID of the project where the backend server group is used. Range: N/A
protocol	String	Definition: Specifies the protocol used by the backend server group to receive requests. Range: The value can be TCP , UDP , QUIC , or TLS .
session_persistence	SessionPersistence object	Definition: Specifies the sticky session.
ip_version	String	Definition: Specifies the IP address version supported by the backend server group. 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.
created_at	String	Definition: Specifies the creation time. The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Range: N/A Note: This parameter 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	Definition: Specifies the update time. The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Range: N/A Note: This parameter 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	Definition: Specifies the ID of the VPC where the backend server group works. Range: N/A
type	String	Definition: Specifies the backend server group type. Range: • 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	Definition: Specifies the ID of the enterprise project. Range: • 0: The resource belongs to the default enterprise project. • A string in UUID format indicates a non-default enterprise project.
healthmonitor	MasterSlaveHealthMonitor object	Definition: Specifies the health check configured for the active/standby backend server group.

Parameter	Type	Description
any_port_enable	Boolean	Definition: 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 . Range: false (disable this option) or true (enable this option).
connection_drain	ConnectionDrain object	Definition: Specifies the configurations of deregistration delay. 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. Range: N/A
quic_cid_hash_strategy	QuicCidHashStrategy object	Definition: Specifies multi-path distribution configuration based on destination connection IDs.

Table 5-702 ListenerRef

Parameter	Type	Description
id	String	Definition: Specifies the listener ID. Range: N/A

Table 5-703 LoadBalancerRef

Parameter	Type	Description
id	String	Definition: Specifies the load balancer ID. Range: N/A

Table 5-704 MasterSlaveMember

Parameter	Type	Description
id	String	Specifies the backend server ID. Range: N/A
name	String	Definition: Specifies the backend server name. Range: N/A
admin_state_up	Boolean	Definition: Specifies the administrative status of the backend server. 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 . Range: true or false
subnet_cidr_id	String	Specifies the ID of the IPv4 or IPv6 subnet where the backend server works. If ip_target_enable is set to true , this parameter can be left blank, indicating that an IP as backend server will be added. 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. Range: N/A
protocol_port	Integer	Definition: 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	Definition: Specifies the IP address of the backend server Range: N/A
ip_version	String	Definition: Specifies the IP address version supported by the backend server. The version depends on the value of address returned by the system. Range: v4 or v6

Parameter	Type	Description
device_owner	String	Definition: Specifies whether the backend server is associated with an ECS. Range: - 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	Definition: 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. Range: N/A This parameter is unsupported. Please do not use it.
operating_status	String	Definition: Specifies the operating status of the backend server if listener_id under status is not specified. Range: 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	Definition: Specifies why the health check fails.

Parameter	Type	Description
member_type	String	Definition: Specifies the type of the backend server. Range: • ip: IP as backend servers • instance: ECSs used as backend servers
instance_id	String	Definition: 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. Range: N/A
role	String	Definition: Specifies the type of the backend server. Range: N/A
status	Array of ListenerMemberInfo objects	Definition: 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. Range: N/A

Table 5-705 MemberHealthCheckFailedReason

Parameter	Type	Description
reason_code	String	Definition: Specifies the code of the health check failures. Range: • 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	Definition: 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. 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. • 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	Definition: 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. 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 5-706 ListenerMemberInfo

Parameter	Type	Description
listener_id	String	Definition: Specifies the ID of the listener associated with the backend server. Range: N/A
operating_status	String	Definition: Specifies the operating status of the backend server. Range: • 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 5-707 SessionPersistence

Parameter	Type	Description
cookie_name	String	Definition: Specifies the cookie name. Range: The value can contain a maximum of 1,024 characters.
type	String	Definition: Specifies the sticky session type. Range: SOURCE_IP , HTTP_COOKIE , or APP_COOKIE .
persistence_timeout	Integer	Definition: Specifies the stickiness duration, in minutes. This parameter will not take effect when type is set to APP_COOKIE . Range: • 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 5-708 MasterSlaveHealthMonitor

Parameter	Type	Description
admin_state_up	Boolean	Definition: Specifies the administrative status of the health check. Range: • true: The health check function is enabled. • false: The health check function is disabled.
delay	Integer	Definition: Specifies the interval between health checks, in seconds. Range: 1 to 50
domain_name	String	Definition: Specifies the domain name that HTTP requests are sent to during the health check. Range: The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter.
expected_codes	String	Definition: Specifies the expected HTTP status code. Range: • 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	String	Definition: Specifies the HTTP method. Range: GET, HEAD, or POST
id	String	Specifies the health check ID. Default value: N/A
max_retries	Integer	Definition: Specifies the number of consecutive health checks when the health check result of a backend server changes from OFFLINE to ONLINE . Range: 1 to 10
max_retries_down	Integer	Definition: Specifies the number of consecutive health checks when the health check result of a backend server changes from ONLINE to OFFLINE . Range: 1 to 10

Parameter	Type	Description
monitor_port	Integer	Specifies the port used for the health check. Range: 1 to 65535
name	String	Definition: Specifies the health check name. Range: N/A
timeout	Integer	Definition: Specifies the maximum time required for waiting for a response from the health check, in seconds. Range: N/A
type	String	Definition: Specifies the health check protocol. Range: The value can be TCP , UDP_CONNECT , HTTP , or HTTPS .
url_path	String	Definition: Specifies the HTTP request path for the health check. The value must start with a slash (/), and the default value is /. Range: The value can contain letters, digits, hyphens (-), slashes (/), periods (.), percentage signs (%), question marks (?), pound signs (#), ampersand signs (&), and the extended character set: _~!()*[]@\$^'+.

Table 5-709 ConnectionDrain

Parameter	Type	Description
enable	Boolean	Definition: Specifies whether to enable connection_drain . Constraints: N/A Range: The value can be true (enable this option) or false (disable this option). Default value: N/A
timeout	Integer	Definition: Specifies the deregistration delay timeout, in seconds. Constraints: N/A Range: 10 to 4000, in seconds. Constraints: N/A

Table 5-710 QuicCidHashStrategy

Parameter	Type	Description
len	Integer	Definition: Specifies the length of the hash factor in the connection ID. Constraints: This parameter is valid only when the load balancing algorithm is QUIC_CID . Range: 1 to 20 Default value: 3
offset	Integer	Definition: Specifies the start position in the connection ID as the hash factor. Constraints: This parameter is valid only when the load balancing algorithm is QUIC_CID . 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

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": [ {
        "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	Successful request.

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 5-711 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Table 5-712 Query Parameters

Parameter	Mandatory	Type	Description
marker	No	String	Definition: Specifies the ID of the last record on the previous page. Constraints: • This parameter must be used together with limit. • If the parameter is not specified, only resources on the first page are queried. • This parameter cannot be left blank or set to an invalid ID. Range: N/A Default value: N/A
limit	No	Integer	Definition: Specifies the number of records returned on each page. Constraints: N/A Range: 0 to 2000 Default value: 2000
page_reverse	No	Boolean	Definition: Specifies whether to use reverse query. Constraints: • This parameter must be used together with limit. • If page_reverse is set to true and you want to query the resources on the previous page, set the value of marker to the value of previous_marker. Range: • true: Query resources on the previous page. • false: Query resources on the next page. Default value: false

Parameter	Mandatory	Type	Description
description	No	Array of strings	Definition: Specifies the supplementary information about the backend server group. Multiple descriptions can be used for query in the format of <i>description=xxx&description=xx</i> . Constraints: N/A Range: N/A Default value: N/A
healthmonitor_id	No	Array of strings	Definition: Specifies the ID of the health check configured for the backend server group. Multiple IDs can be used for query in the format of <i>healthmonitor_id=xxx&healthmonitor_id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
id	No	Array of strings	Definition: Specifies the ID of the backend server group. Multiple IDs can be used for query in the format of <i>id=xxx&id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
name	No	Array of strings	Definition: Specifies the name of the active/standby backend server group. Multiple names can be used for query in the format of <i>name=xxx&name=xxx</i> . Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
loadbalancer_id	No	Array of strings	Definition: Specifies the ID of the load balancer with which the backend server group is associated. Multiple IDs can be used for query in the format of <i>loadbalancer_id=xxx&loadbalancer_id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
protocol	No	Array of strings	Definition: Specifies the protocol used by the backend server group to receive requests from the load balancer. Multiple protocols can be used for query in the format of <i>protocol=xxx&protocol=xxx</i> . Constraints: N/A Range: The value can be TCP , UDP , TLS , HTTP , HTTPS , GRPC , or QUIC . Default value: N/A
lb_algorithm	No	Array of strings	Definition: Specifies the load balancing algorithm used by the load balancer to route requests to backend servers in the associated backend server group. Multiple algorithms can be used for query in the format of <i>lb_algorithm=xxx&lb_algorithm=xxx</i> . Constraints: N/A Range: ● ROUND_ROBIN: weighted round robin ● LEAST_CONNECTIONS: weighted least connections ● SOURCE_IP: source IP hash ● QUIC_CID: connection ID Default value: N/A

Parameter	Mandatory	Type	Description
enterprise_project_id	No	Array of strings	Definition: Specifies the ID of the enterprise project. Multiple values can be used for query in the format of: <i>enterprise_project_id=xxx&enterprise_project_id=xxx.</i> Constraints: • If enterprise_project_id is not specified, resources in all enterprise projects are queried by default. Fine-grained authorization is performed. The elb:poools: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:poools:list permission are queried. Range: N/A Default value: N/A
ip_version	No	Array of strings	Definition: Specifies the IP address version supported by the backend server group. Multiple versions can be used for query in the format of <i>ip_version=xxx&ip_version=xxx.</i> Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
member_address	No	Array of strings	Definition: Specifies the IP address of the backend server. Multiple IP addresses can be used for query in the format of <i>member_address=xxx&member_address=xxx</i> . Constraints: This is a query parameter and will not be included in the response. Range: N/A Default value: N/A
member_device_id	No	Array of strings	Definition: Specifies the ID of the ECS that is associated with the load balancer as a backend server. Multiple IDs can be used for query in the format of <i>member_device_id=xxx&member_device_id=xxx</i> . Constraints: This is a query parameter and will not be included in the response. Range: N/A Default value: N/A
listener_id	No	Array of strings	Definition: Specifies the IDs of the associated listeners, including the listeners associated through forwarding policies. Multiple IDs can be used for query in the format of <i>listener_id=xxx&listener_id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
member_instance_id	No	Array of strings	Definition: Specifies the backend server ID. Multiple IDs can be used for query in the format of <i>member_instance_id=xxx&member_instance_id=xxx</i> . Constraints: This is a query parameter and will not be included in the response. Range: N/A Default value: N/A
vpc_id	No	Array of strings	Definition: Specifies the ID of the VPC where the backend server group works. Constraints: N/A Range: N/A Default value: N/A
type	No	Array of strings	Definition: Specifies the type of the backend server group. Constraints: N/A Range: • 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. Default value: N/A
connection_drain	No	Boolean	Specifies a connection_drain value for query, in the format of connection_drain=true or connection_drain=false . Constraints: N/A Range: The value can be true (enabled) or false (disabled). Default value: N/A

Request Parameters

Table 5-713 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200**Table 5-714** Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
page_info	PageInfo object	Definition: Specifies the pagination information.
pools	Array of MasterSlavePool objects	Definition: Specifies the backend server groups.

Table 5-715 PageInfo

Parameter	Type	Description
previous_marker	String	Definition: Specifies the ID of the first record in the pagination query result. If page_reverse is set to true , this parameter is used together to query resources on the previous page. Range: N/A

Parameter	Type	Description
next_marker	String	Definition: Specifies the ID of the last record in the pagination query result. It is usually used to query resources on the next page. Range: N/A
current_count	Integer	Definition: Specifies the number of records returned on the current page. Range: N/A

Table 5-716 MasterSlavePool

Parameter	Type	Description
description	String	Definition: Specifies the supplementary information about the backend server group. Range: N/A
id	String	Definition: Specifies the ID of the backend server group. Range: N/A
lb_algorithm	String	Definition: Specifies the load balancing algorithm used by the load balancer to route requests to backend servers in the associated backend server group. Range: • ROUND_ROBIN: weighted round robin • LEAST_CONNECTIONS: weighted least connections • SOURCE_IP: source IP hash • QUIC_CID: connection ID
listeners	Array of ListenerRef objects	Definition: Specifies the IDs of the listeners with which the backend server group is associated.
loadbalancers	Array of LoadBalancerRef objects	Definition: Specifies the IDs of the load balancers with which the active/standby backend server group is associated.
members	Array of MasterSlaveMember objects	Definition: Specifies the backend servers in the backend server group.

Parameter	Type	Description
name	String	Definition: Specifies the backend server group name. Range: N/A
project_id	String	Definition: Specifies the ID of the project where the backend server group is used. Range: N/A
protocol	String	Definition: Specifies the protocol used by the backend server group to receive requests. Range: The value can be TCP , UDP , QUIC , or TLS .
session_persistence	SessionPersistence object	Definition: Specifies the sticky session.
ip_version	String	Definition: Specifies the IP address version supported by the backend server group. 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.
created_at	String	Definition: Specifies the creation time. The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Range: N/A Note: This parameter 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	Definition: Specifies the update time. The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Range: N/A Note: This parameter 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	Definition: Specifies the ID of the VPC where the backend server group works. Range: N/A
type	String	Definition: Specifies the backend server group type. Range: • 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	Definition: Specifies the ID of the enterprise project. Range: • 0: The resource belongs to the default enterprise project. • A string in UUID format indicates a non-default enterprise project.
healthmonitor	MasterSlaveHealthMonitor object	Definition: Specifies the health check configured for the active/standby backend server group.

Parameter	Type	Description
any_port_enable	Boolean	Definition: 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 . Range: false (disable this option) or true (enable this option).
connection_drain	ConnectionDrain object	Definition: Specifies the configurations of deregistration delay. 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. Range: N/A
quic_cid_hash_strategy	QuicCidHashStrategy object	Definition: Specifies multi-path distribution configuration based on destination connection IDs.

Table 5-717 ListenerRef

Parameter	Type	Description
id	String	Definition: Specifies the listener ID. Range: N/A

Table 5-718 LoadBalancerRef

Parameter	Type	Description
id	String	Definition: Specifies the load balancer ID. Range: N/A

Table 5-719 MasterSlaveMember

Parameter	Type	Description
id	String	Specifies the backend server ID. Range: N/A
name	String	Definition: Specifies the backend server name. Range: N/A
admin_state_up	Boolean	Definition: Specifies the administrative status of the backend server. 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 . Range: true or false
subnet_cidr_id	String	Specifies the ID of the IPv4 or IPv6 subnet where the backend server works. If ip_target_enable is set to true , this parameter can be left blank, indicating that an IP as backend server will be added. 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. Range: N/A
protocol_port	Integer	Definition: 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	Definition: Specifies the IP address of the backend server Range: N/A
ip_version	String	Definition: Specifies the IP address version supported by the backend server. The version depends on the value of address returned by the system. Range: v4 or v6

Parameter	Type	Description
device_owner	String	Definition: Specifies whether the backend server is associated with an ECS. Range: - 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	Definition: 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. Range: N/A This parameter is unsupported. Please do not use it.
operating_status	String	Definition: Specifies the operating status of the backend server if listener_id under status is not specified. Range: 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	Definition: Specifies why the health check fails.

Parameter	Type	Description
member_type	String	Definition: Specifies the type of the backend server. Range: • ip: IP as backend servers • instance: ECSs used as backend servers
instance_id	String	Definition: 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. Range: N/A
role	String	Definition: Specifies the type of the backend server. Range: N/A
status	Array of ListenerMemberInfo objects	Definition: 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. Range: N/A

Table 5-720 MemberHealthCheckFailedReason

Parameter	Type	Description
reason_code	String	Definition: Specifies the code of the health check failures. Range: • 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	Definition: 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. 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. • 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	Definition: 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. 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 5-721 ListenerMemberInfo

Parameter	Type	Description
listener_id	String	Definition: Specifies the ID of the listener associated with the backend server. Range: N/A
operating_status	String	Definition: Specifies the operating status of the backend server. Range: • 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 5-722 SessionPersistence

Parameter	Type	Description
cookie_name	String	Definition: Specifies the cookie name. Range: The value can contain a maximum of 1,024 characters.
type	String	Definition: Specifies the sticky session type. Range: SOURCE_IP , HTTP_COOKIE , or APP_COOKIE .
persistence_timeout	Integer	Definition: Specifies the stickiness duration, in minutes. This parameter will not take effect when type is set to APP_COOKIE . Range: • 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 5-723 MasterSlaveHealthMonitor

Parameter	Type	Description
admin_state_up	Boolean	Definition: Specifies the administrative status of the health check. Range: • true: The health check function is enabled. • false: The health check function is disabled.
delay	Integer	Definition: Specifies the interval between health checks, in seconds. Range: 1 to 50
domain_name	String	Definition: Specifies the domain name that HTTP requests are sent to during the health check. Range: The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter.
expected_codes	String	Definition: Specifies the expected HTTP status code. Range: • 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	String	Definition: Specifies the HTTP method. Range: GET, HEAD, or POST
id	String	Specifies the health check ID. Default value: N/A
max_retries	Integer	Definition: Specifies the number of consecutive health checks when the health check result of a backend server changes from OFFLINE to ONLINE . Range: 1 to 10
max_retries_down	Integer	Definition: Specifies the number of consecutive health checks when the health check result of a backend server changes from ONLINE to OFFLINE . Range: 1 to 10

Parameter	Type	Description
monitor_port	Integer	Specifies the port used for the health check. Range: 1 to 65535
name	String	Definition: Specifies the health check name. Range: N/A
timeout	Integer	Definition: Specifies the maximum time required for waiting for a response from the health check, in seconds. Range: N/A
type	String	Definition: Specifies the health check protocol. Range: The value can be TCP , UDP_CONNECT , HTTP , or HTTPS .
url_path	String	Definition: Specifies the HTTP request path for the health check. The value must start with a slash (/), and the default value is /. Range: The value can contain letters, digits, hyphens (-), slashes (/), periods (.), percentage signs (%), question marks (?), pound signs (#), ampersand signs (&), and the extended character set: _~!()*[]@\$^'+.

Table 5-724 ConnectionDrain

Parameter	Type	Description
enable	Boolean	Definition: Specifies whether to enable connection_drain . Constraints: N/A Range: The value can be true (enable this option) or false (disable this option). Default value: N/A
timeout	Integer	Definition: Specifies the deregistration delay timeout, in seconds. Constraints: N/A Range: 10 to 4000, in seconds. Constraints: N/A

Table 5-725 QuicCidHashStrategy

Parameter	Type	Description
len	Integer	Definition: Specifies the length of the hash factor in the connection ID. Constraints: This parameter is valid only when the load balancing algorithm is QUIC_CID . Range: 1 to 20 Default value: 3
offset	Integer	Definition: Specifies the start position in the connection ID as the hash factor. Constraints: This parameter is valid only when the load balancing algorithm is QUIC_CID . 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.getenv("CLOUD_SDK_AK")
    sk = os.getenv("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 5-726 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
pool_id	Yes	String	Definition: Specifies the backend server group ID. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-727 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-728 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
pool	MasterSlavePool object	Definition: Specifies the backend server group.

Table 5-729 MasterSlavePool

Parameter	Type	Description
description	String	Definition: Specifies the supplementary information about the backend server group. Range: N/A
id	String	Definition: Specifies the ID of the backend server group. Range: N/A

Parameter	Type	Description
lb_algorithm	String	Definition: Specifies the load balancing algorithm used by the load balancer to route requests to backend servers in the associated backend server group. Range: • ROUND_ROBIN: weighted round robin • LEAST_CONNECTIONS: weighted least connections • SOURCE_IP: source IP hash • QUIC_CID: connection ID
listeners	Array of ListenerRef objects	Definition: Specifies the IDs of the listeners with which the backend server group is associated.
loadbalancers	Array of LoadBalancerRef objects	Definition: Specifies the IDs of the load balancers with which the active/standby backend server group is associated.
members	Array of MasterSlaveMember objects	Definition: Specifies the backend servers in the backend server group.
name	String	Definition: Specifies the backend server group name. Range: N/A
project_id	String	Definition: Specifies the ID of the project where the backend server group is used. Range: N/A
protocol	String	Definition: Specifies the protocol used by the backend server group to receive requests. Range: The value can be TCP , UDP , QUIC , or TLS .
session_persistence	SessionPersistence object	Definition: Specifies the sticky session.

Parameter	Type	Description
ip_version	String	Definition: Specifies the IP address version supported by the backend server group. 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.
created_at	String	Definition: Specifies the creation time. The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Range: N/A Note: This parameter 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	Definition: Specifies the update time. The value must be a UTC time in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Range: N/A Note: This parameter 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	Definition: Specifies the ID of the VPC where the backend server group works. Range: N/A

Parameter	Type	Description
type	String	Definition: Specifies the backend server group type. Range: • 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	Definition: Specifies the ID of the enterprise project. Range: • 0: The resource belongs to the default enterprise project. • A string in UUID format indicates a non-default enterprise project.
healthmonitor	MasterSlaveHealthMonitor object	Definition: Specifies the health check configured for the active/standby backend server group.
any_port_enable	Boolean	Definition: 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 . Range: false (disable this option) or true (enable this option).
connection_drain	ConnectionDrain object	Definition: Specifies the configurations of deregistration delay. 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. Range: N/A

Parameter	Type	Description
quic_cid_hash_strategy	QuicCidHashStrategy object	Definition: Specifies multi-path distribution configuration based on destination connection IDs.

Table 5-730 ListenerRef

Parameter	Type	Description
id	String	Definition: Specifies the listener ID. Range: N/A

Table 5-731 LoadBalancerRef

Parameter	Type	Description
id	String	Definition: Specifies the load balancer ID. Range: N/A

Table 5-732 MasterSlaveMember

Parameter	Type	Description
id	String	Specifies the backend server ID. Range: N/A
name	String	Definition: Specifies the backend server name. Range: N/A
admin_state_up	Boolean	Definition: Specifies the administrative status of the backend server. 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 . Range: true or false

Parameter	Type	Description
subnet_cidr_id	String	Specifies the ID of the IPv4 or IPv6 subnet where the backend server works. If ip_target_enable is set to true, this parameter can be left blank, indicating that an IP as backend server will be added. 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. Range: N/A
protocol_port	Integer	Definition: 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	Definition: Specifies the IP address of the backend server Range: N/A
ip_version	String	Definition: Specifies the IP address version supported by the backend server. The version depends on the value of address returned by the system. Range: v4 or v6
device_owner	String	Definition: Specifies whether the backend server is associated with an ECS. Range: • 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.

Parameter	Type	Description
device_id	String	Definition: 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. Range: N/A This parameter is unsupported. Please do not use it.
operating_status	String	Definition: Specifies the operating status of the backend server if listener_id under status is not specified. Range: • 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	Definition: Specifies why the health check fails.
member_type	String	Definition: Specifies the type of the backend server. Range: • ip: IP as backend servers • instance: ECSs used as backend servers
instance_id	String	Definition: 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. Range: N/A
role	String	Definition: Specifies the type of the backend server. Range: N/A

Parameter	Type	Description
status	Array of ListenerMemberInfo objects	Definition: 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. Range: N/A

Table 5-733 MemberHealthCheckFailedReason

Parameter	Type	Description
reason_code	String	Definition: Specifies the code of the health check failures. Range: • 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	Definition: 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. 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. • 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	Definition: 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. 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 5-734 ListenerMemberInfo

Parameter	Type	Description
listener_id	String	Definition: Specifies the ID of the listener associated with the backend server. Range: N/A
operating_status	String	Definition: Specifies the operating status of the backend server. Range: • 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 5-735 SessionPersistence

Parameter	Type	Description
cookie_name	String	Definition: Specifies the cookie name. Range: The value can contain a maximum of 1,024 characters.
type	String	Definition: Specifies the sticky session type. Range: SOURCE_IP , HTTP_COOKIE , or APP_COOKIE .
persistence_timeout	Integer	Definition: Specifies the stickiness duration, in minutes. This parameter will not take effect when type is set to APP_COOKIE . Range: • 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 5-736 MasterSlaveHealthMonitor

Parameter	Type	Description
admin_state_up	Boolean	Definition: Specifies the administrative status of the health check. Range: • true: The health check function is enabled. • false: The health check function is disabled.
delay	Integer	Definition: Specifies the interval between health checks, in seconds. Range: 1 to 50
domain_name	String	Definition: Specifies the domain name that HTTP requests are sent to during the health check. Range: The value can contain only digits, letters, hyphens (-), and periods (.) and must start with a digit or letter.
expected_codes	String	Definition: Specifies the expected HTTP status code. Range: • 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	String	Definition: Specifies the HTTP method. Range: GET, HEAD, or POST
id	String	Specifies the health check ID. Default value: N/A
max_retries	Integer	Definition: Specifies the number of consecutive health checks when the health check result of a backend server changes from OFFLINE to ONLINE . Range: 1 to 10
max_retries_down	Integer	Definition: Specifies the number of consecutive health checks when the health check result of a backend server changes from ONLINE to OFFLINE . Range: 1 to 10

Parameter	Type	Description
monitor_port	Integer	Specifies the port used for the health check. Range: 1 to 65535
name	String	Definition: Specifies the health check name. Range: N/A
timeout	Integer	Definition: Specifies the maximum time required for waiting for a response from the health check, in seconds. Range: N/A
type	String	Definition: Specifies the health check protocol. Range: The value can be TCP , UDP_CONNECT , HTTP , or HTTPS .
url_path	String	Definition: Specifies the HTTP request path for the health check. The value must start with a slash (/), and the default value is /. Range: The value can contain letters, digits, hyphens (-), slashes (/), periods (.), percentage signs (%), question marks (?), pound signs (#), ampersand signs (&), and the extended character set: _~!()*[]@\$^'+.

Table 5-737 ConnectionDrain

Parameter	Type	Description
enable	Boolean	Definition: Specifies whether to enable connection_drain . Constraints: N/A Range: The value can be true (enable this option) or false (disable this option). Default value: N/A
timeout	Integer	Definition: Specifies the deregistration delay timeout, in seconds. Constraints: N/A Range: 10 to 4000, in seconds. Constraints: N/A

Table 5-738 QuicCidHashStrategy

Parameter	Type	Description
len	Integer	Definition: Specifies the length of the hash factor in the connection ID. Constraints: This parameter is valid only when the load balancing algorithm is QUIC_CID . Range: 1 to 20 Default value: 3
offset	Integer	Definition: Specifies the start position in the connection ID as the hash factor. Constraints: This parameter is valid only when the load balancing algorithm is QUIC_CID . 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 5-739 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
pool_id	Yes	String	Definition: Specifies the backend server group ID. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-740 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 204

Successful request.

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 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	Successful request.

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 5-741 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-742 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-743 Request body parameters

Parameter	Mandatory	Type	Description
logtank	Yes	CreateLogtankOption object	Definition: Specifies the request parameters for creating a log. Constraints: N/A

Table 5-744 CreateLogtankOption

Parameter	Mandatory	Type	Description
loadbalancer_id	Yes	String	Definition: Specifies the load balancer ID. Constraints: N/A Range: N/A Default value: N/A
log_group_id	Yes	String	Definition: Specifies the log group ID. This parameter is available for all services other than ELB. Constraints: N/A Range: N/A Default value: N/A
log_topic_id	Yes	String	Definition: Specifies the ID of the log subscription topic. This parameter is available for all services other than ELB. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 201

Table 5-745 Response body parameters

Parameter	Type	Description
logtank	Logtank object	Definition: Provides supplementary information.

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

Table 5-746 Logtank

Parameter	Type	Description
id	String	Definition: Specifies the log ID. Range: N/A
project_id	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Range: The value can contain a maximum of 32 characters, including digits and lowercase letters.
loadbalancer_id	String	Definition: Specifies the load balancer ID. Range: N/A
log_group_id	String	Definition: Specifies the log group ID. Range: N/A
log_topic_id	String	Definition: Specifies the log topic ID. Range: N/A

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 5-747 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Table 5-748 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Definition: Specifies the number of records returned on each page. Constraints: N/A Range: 0 to 2000 Default value: 2000

Parameter	Mandatory	Type	Description
marker	No	String	Definition: Specifies the ID of the last record on the previous page. Constraints: • This parameter must be used together with limit. • If the parameter is not specified, only resources on the first page are queried. • This parameter cannot be left blank or set to an invalid ID. Range: N/A Default value: N/A
page_reverse	No	Boolean	Definition: Specifies whether to use reverse query. Constraints: • This parameter must be used together with limit. • If page_reverse is set to true and you want to query the resources on the previous page, set the value of marker to the value of previous_marker. Range: • true: Query resources on the previous page. • false: Query resources on the next page. Default value: false

Parameter	Mandatory	Type	Description
enterprise_project_id	No	Array of strings	Definition: Specifies the ID of the enterprise project. Multiple values can be used for query in the format of: <i>enterprise_project_id=xxx&enterprise_project_id=xxx.</i> Constraints: • 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. Range: N/A Default value: N/A
id	No	Array of strings	Definition: Specifies the ID of the log tank. Multiple IDs can be used for query in the format of <i>id=xxx&id=xxx.</i> Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
loadbalancer_id	No	Array of strings	Definition: Specifies the ID of the load balancer. Multiple IDs can be used for query in the format of <i>loadbalancer_id=xxx&loadbalancer_id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
log_group_id	No	Array of strings	Definition: Specifies the log group ID. Multiple IDs can be used for query in the format of <i>log_group_id=xxx&log_group_id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A
log_topic_id	No	Array of strings	Definition: Specifies the log topic ID. Multiple IDs can be used for query in the format of <i>log_topic_id=xxx&log_topic_id=xxx</i> . Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-749 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-750 Response body parameters

Parameter	Type	Description
logtanks	Array of Logtank objects	Definition: Provides supplementary information.
page_info	PageInfo object	Definition: Specifies the pagination information.
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

Table 5-751 Logtank

Parameter	Type	Description
id	String	Definition: Specifies the log ID. Range: N/A
project_id	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Range: The value can contain a maximum of 32 characters, including digits and lowercase letters.
loadbalancer_id	String	Definition: Specifies the load balancer ID. Range: N/A
log_group_id	String	Definition: Specifies the log group ID. Range: N/A
log_topic_id	String	Definition: Specifies the log topic ID. Range: N/A

Table 5-752 PageInfo

Parameter	Type	Description
previous_marker	String	Definition: Specifies the ID of the first record in the pagination query result. If page_reverse is set to true , this parameter is used together to query resources on the previous page. Range: N/A
next_marker	String	Definition: Specifies the ID of the last record in the pagination query result. It is usually used to query resources on the next page. Range: N/A
current_count	Integer	Definition: Specifies the number of records returned on the current page. Range: N/A

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

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from 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.ElClientBuilder().
            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 5-753 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
logtank_id	Yes	String	Definition: Specifies the log ID. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-754 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200**Table 5-755** Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
logtank	Logtank object	Definition: Provides supplementary information about the log.

Table 5-756 Logtank

Parameter	Type	Description
id	String	Definition: Specifies the log ID. Range: N/A
project_id	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Range: The value can contain a maximum of 32 characters, including digits and lowercase letters.
loadbalancer_id	String	Definition: Specifies the load balancer ID. Range: N/A

Parameter	Type	Description
log_group_id	String	Definition: Specifies the log group ID. Range: N/A
log_topic_id	String	Definition: Specifies the log topic ID. Range: N/A

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 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 5-757 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
logtank_id	Yes	String	Definition: Specifies the log ID. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-758 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-759 Request body parameters

Parameter	Mandatory	Type	Description
logtank	Yes	UpdateLogtankOption object	Definition: Specifies the request parameters for updating a log. Constraints: N/A

Table 5-760 UpdateLogtankOption

Parameter	Mandatory	Type	Description
log_group_id	No	String	Definition: Specifies the log group ID. This parameter is available for all services other than ELB. Constraints: N/A Range: N/A Default value: N/A
log_topic_id	No	String	Definition: Specifies the ID of the log subscription topic. This parameter is available for all services other than ELB. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-761 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
logtank	Logtank object	Definition: Specifies the log information. Range: N/A

Table 5-762 Logtank

Parameter	Type	Description
id	String	Definition: Specifies the log ID. Range: N/A
project_id	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Range: The value can contain a maximum of 32 characters, including digits and lowercase letters.
loadbalancer_id	String	Definition: Specifies the load balancer ID. Range: N/A
log_group_id	String	Definition: Specifies the log group ID. Range: N/A
log_topic_id	String	Definition: Specifies the log topic ID. Range: N/A

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.getStatusCode());
            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 huaweicloudskgelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskgelb.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 5-763 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
logtank_id	Yes	String	Definition: Specifies the log ID. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-764 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 204
No Content
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 huaweicloudskelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskelb.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.ElClientBuilder().
            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 asynchronous tasks like copying or upgrading load balancers.

Calling Method

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

URI

GET /v3/{project_id}/elb/jobs

Table 5-765 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Table 5-766 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Definition: Specifies the number of records returned on each page. Constraints: N/A Range: 0 to 2000 Default value: 2000
marker	No	String	Definition: Specifies the ID of the last record on the previous page. Constraints: • This parameter must be used together with limit. • If the parameter is not specified, only resources on the first page are queried. • This parameter cannot be left blank or set to an invalid ID. Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
page_reverse	No	Boolean	Definition: Specifies whether to use reverse query. Constraints: • This parameter must be used together with limit. • If page_reverse is set to true and you want to query the resources on the previous page, set the value of marker to the value of previous_marker. Range: • true: Query resources on the previous page. • false: Query resources on the next page. Default value: false
job_id	No	String	Definition: Specifies the task ID. Constraints: N/A Range: N/A Default value: N/A
job_type	No	String	Definition: Specifies the task type. Constraints: N/A Range: N/A Default value: N/A
status	No	String	Definition: Specifies the task status. Constraints: N/A Range: INIT, RUNNING, FAIL, SUCCESS, ROLLBACKING, COMPLETE, ROLLBACK_FAIL, or CANCEL Default value: N/A
error_code	No	String	Definition: Specifies the task error code. Constraints: N/A Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
resource_id	No	String	Definition: Specifies the resource ID. Constraints: N/A Range: N/A Default value: N/A
project_id	No	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
begin_time	No	String	Definition: Specifies the time when the task started, in the format of <i>yyyy-MM-dd'T'HH:mm:ss</i> . The tasks that started on or after the specified time will be returned. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

None

Response Parameters

Status code: 200

Table 5-767 Response body parameters

Parameter	Type	Description
jobs	Array of MainJob objects	Definition: Specifies the task list.
page_info	PageInfo object	Definition: Specifies the pagination information.

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

Table 5-768 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	Definition: Specifies the resource ID.
sub_jobs	Array of SubJob objects	Definition: Specifies the subtask list.

Table 5-769 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.

Parameter	Type	Description
error_msg	String	Specifies the task error message.
project_id	String	Specifies the project ID.
resource_id	String	Definition: Specifies the resource ID.
entities	Array of JobEntities objects	Definition: Specifies the resource to be processed in a subtask.

Table 5-770 JobEntities

Parameter	Type	Description
resource_id	String	Definition: Specifies the ID of the resource associated with a subtask. Range: N/A
resource_type	String	Definition: Specifies the type of the resource associated with a subtask. Range: N/A

Table 5-771 PageInfo

Parameter	Type	Description
previous_marker	String	Definition: Specifies the ID of the first record in the pagination query result. If page_reverse is set to true , this parameter is used together to query resources on the previous page. Range: N/A
next_marker	String	Definition: Specifies the ID of the last record in the pagination query result. It is usually used to query resources on the next page. Range: N/A
current_count	Integer	Definition: Specifies the number of records returned on the current page. Range: N/A

Example Requests

```
https://{ELB_Endpoint}/v3/7b7705dce1e847b08b3b16dda67fec24/elb/jobs
```

Example Responses

Status code: 200

Query succeeded.

```
{
  "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"
  } ],
  "page_info" : {
    "previous_marker" : "ef6da45b-35d9-4c18-8c35-0b80d94ab9e6",
    "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 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](#).

5.18.2 Querying the Status of an Asynchronous Task

Function

This API is used to query the status of an asynchronous task like copying or upgrading a load balancer.

Calling Method

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

URI

GET /v3/{project_id}/elb/jobs/{job_id}

Table 5-772 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
job_id	Yes	String	Specifies the task ID.

Request Parameters

None

Response Parameters

Status code: 200

Table 5-773 Response body parameters

Parameter	Type	Description
job	MainJob object	Definition: Specifies the information about the asynchronous tasks such as copy tasks.
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

Table 5-774 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	Definition: Specifies the resource ID.
sub_jobs	Array of SubJob objects	Definition: Specifies the subtask list.

Table 5-775 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	Definition: Specifies the resource ID.
entities	Array of JobEntities objects	Definition: Specifies the resource to be processed in a subtask.

Table 5-776 JobEntities

Parameter	Type	Description
resource_id	String	Definition: Specifies the ID of the resource associated with a subtask. Range: N/A
resource_type	String	Definition: Specifies the type of the resource associated with a subtask. Range: N/A

Example Requests

https://{ELB_Endpoint}/v3/7b7705dce1e847b08b3b16dda67fec24/elb/jobs/37d5c1fd-fa57-4c6d-bdcd-d523095c05e8

Example Responses

Status code: 200

Query succeeded.

{
 "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"
}
```

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.getenv("CLOUD_SDK_AK")
    sk = os.getenv("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](#).

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 5-777 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Table 5-778 Query Parameters

Parameter	Mandatory	Type	Description
feature	No	String	Definition: Specifies the feature name. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

None

Response Parameters

Status code: 200

Table 5-779 Response body parameters

Parameter	Type	Description
configs	Array of FeatureConfig objects	Definition: Specifies the feature configuration list.
page_info	PageInfo object	Definition: Specifies the pagination information.
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

Table 5-780 FeatureConfig

Parameter	Type	Description
id	String	Definition: Specifies the configuration ID. Range: N/A
created_at	String	Definition: Specifies the creation time. Range: N/A
updated_at	String	Definition: Specifies the update time. Range: N/A

Parameter	Type	Description
service	String	Definition: Specifies the service. The value is fixed at ELB . Range: N/A
tenant_id	String	Definition: Specifies the tenant ID, which has the same meaning as that of project_id . Range: N/A
feature	String	Definition: Specifies the feature name. Range: N/A
switch	Boolean	Definition: Specifies whether to enable the feature configuration. Range: • true: Enable the feature configuration. • false: Disable the feature configuration.
type	String	Definition: Specifies the type of the feature configuration value. For example, INT indicates an integer. Range: N/A
value	String	Definition: 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. Range: N/A
description	String	Definition: Specifies the feature configuration description. Range: N/A
caller	String	Definition: Specifies the configuration creator. Range: N/A

Table 5-781 PageInfo

Parameter	Type	Description
previous_marker	String	Definition: Specifies the ID of the first record in the pagination query result. If page_reverse is set to true , this parameter is used together to query resources on the previous page. Range: N/A
next_marker	String	Definition: Specifies the ID of the last record in the pagination query result. It is usually used to query resources on the next page. Range: N/A
current_count	Integer	Definition: Specifies the number of records returned on the current page. Range: N/A

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

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from 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 5-782 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
loadbalancer_id	Yes	String	Definition: Specifies the load balancer ID. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

None

Response Parameters

Status code: 200

Table 5-783 Response body parameters

Parameter	Type	Description
features	Array of LoadbalancerFeature objects	Definition: Specifies the load balancer feature information list.
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

Table 5-784 LoadbalancerFeature

Parameter	Type	Description
feature	String	Definition: Specifies the feature name. Range: N/A
type	String	Definition: Specifies the type of the feature configuration value. For example, INT indicates an integer. Range: N/A
value	String	Definition: 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. Range: N/A

Example Requests

https://{ELB_Endpoint}/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.getenv("CLOUD_SDK_AK")
    sk = os.getenv("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.ElClientBuilder().
            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 Recycle Bin

5.20.1 Enabling or Disabling Recycle Bin

Function

This API is used to enable or disable recycle bin. Once this option is enabled, deleted load balancers will be kept in the recycle bin. If this option is not enabled, deleted load balancers will be permanently deleted and cannot be restored. Before disabling recycle bin, restore or permanently delete load balancers from the recycle bin.

Calling Method

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

URI

PUT /v3/{project_id}/elb/recycle-bin

Table 5-785 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-786 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-787 Request body parameters

Parameter	Mandatory	Type	Description
recycle_bin	No	RecycleBinRequestBody object	Definition: Request body for updating the value of enable for the recycle bin.

Table 5-788 RecycleBinRequestBody

Parameter	Mandatory	Type	Description
enable	No	Boolean	Definition: Specifies whether to enable recycle bin. Range: • true: Enable recycle bin. • false: Disable recycle bin.

Response Parameters

Status code: 200

Table 5-789 Response body parameters

Parameter	Type	Description
recycle_bin	RecycleBinResponseBody object	Definition: Specifies the response body for the recycle bin.

Table 5-790 RecycleBinResponseBody

Parameter	Type	Description
project_id	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Range: The value can contain a maximum of 32 characters, including digits and lowercase letters.
policy	RecycleBinPolicy object	Definition: Specifies the recycle bin policy.
enable	Boolean	Definition: Specifies whether to enable recycle bin. Range: • true: Enable recycle bin. • false: Disable recycle bin.

Table 5-791 RecycleBinPolicy

Parameter	Type	Description
recycle_threshold_hour	Integer	Definition: Specifies how old a deleted or unsubscribed load balancer has to be for it to be moved to the recycle bin. A load balancer can only be moved to the recycle bin if it has been there longer than the specified number of days in the policy. Range: N/A
retention_hour	Integer	Definition: Specifies how long you want your load balancers to be kept in the recycle bin. Range: N/A

Example Requests

```
https://{ELB_Endpoint}/v3/7b7705dce1e847b08b3b16dda67fec24/elb/recycle-bin
{
  "recycle_bin" : {
    "enable" : false
  }
}
```

Example Responses

Status code: 200

Query succeeded.

```
{
  "recycle_bin" : {
    "enable" : true,
    "policy" : {
      "recycle_threshold_hour" : 20,
      "retention_hour" : 20
    },
    "project_id" : "7b7705dce1e847b08b3b16dda67fec24"
  }
}
```

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 UpdateRecycleBinEnableSolution {

    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();
        UpdateRecycleBinEnableRequest request = new UpdateRecycleBinEnableRequest();
        UpdateRecycleBinEnableRequestBody body = new UpdateRecycleBinEnableRequestBody();
        RecycleBinRequestBody recycleBinbody = new RecycleBinRequestBody();
        recycleBinbody.withEnable(false);
        body.withRecycleBin(recycleBinbody);
        request.withBody(body);
        try {
            UpdateRecycleBinEnableResponse response = client.updateRecycleBinEnable(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getStatusCode());
        }
    }
}
```

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

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from huaweicloudskgelb.v3.region.elb_region import ElbRegion
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudskgelb.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 = UpdateRecycleBinEnableRequest()
        recycleBinbody = RecycleBinRequestBody(
            enable=False
        )
        request.body = UpdateRecycleBinEnableRequestBody(
            recycle_bin=recycleBinbody
        )
        response = client.update_recycle_bin_enable(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.UpdateRecycleBinEnableRequest{}
enableRecycleBin:= false
recycleBinbody := &model.RecycleBinRequestBody{
    Enable: &enableRecycleBin,
}
request.Body = &model.UpdateRecycleBinEnableRequestBody{
    RecycleBin: recycleBinbody,
}
response, err := client.UpdateRecycleBinEnable(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](#).

5.20.2 Querying the Recycle Bin Policy

Function

This API is used to query the recycle bin policy.

Calling Method

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

URI

GET /v3/{project_id}/elb/recycle-bin

Table 5-792 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-793 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-794 Response body parameters

Parameter	Type	Description
recycle_bin	RecycleBinResponseBody object	Definition: Specifies the response body for the recycle bin.

Table 5-795 RecycleBinResponseBody

Parameter	Type	Description
project_id	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Range: The value can contain a maximum of 32 characters, including digits and lowercase letters.
policy	RecycleBinPolicy object	Definition: Specifies the recycle bin policy.
enable	Boolean	Definition: Specifies whether to enable recycle bin. Range: • true: Enable recycle bin. • false: Disable recycle bin.

Table 5-796 RecycleBinPolicy

Parameter	Type	Description
recycle_threshold_hour	Integer	Definition: Specifies how old a deleted or unsubscribed load balancer has to be for it to be moved to the recycle bin. A load balancer can only be moved to the recycle bin if it has been there longer than the specified number of days in the policy. Range: N/A
retention_hour	Integer	Definition: Specifies how long you want your load balancers to be kept in the recycle bin. Range: N/A

Example Requests

```
https://{ELB_Endpoint}/v3/7b7705dce1e847b08b3b16dda67fec24/elb/recycle-bin
```

Example Responses

Status code: 200

Query succeeded.

```
{  
  "recycle_bin" : {  
    "enable" : true,  
    "policy" : {
```

```
"recycle_threshold_hour" : 20,
"retention_hour" : 20
},
"project_id" : "7b7705dce1e847b08b3b16dda67fec24"
}
}
```

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 ShowRecycleBinSolution {

    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();
        ShowRecycleBinRequest request = new ShowRecycleBinRequest();
        try {
            ShowRecycleBinResponse response = client.showRecycleBin(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
            System.out.println(e.getStatusCode());
            System.out.println(e.getRequestId());
            System.out.println(e.getErrorCode());
            System.out.println(e.getErrorMsg());
        }
    }
}
```

Python

```
# coding: utf-8
```

```
import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from 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 = ShowRecycleBinRequest()
        response = client.show_recycle_bin(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.ElClientBuilder().
            WithRegion(region.ValueOf("<YOUR REGION>")).
            WithCredential(auth).
            Build())

    request := &model.ShowRecycleBinRequest{}
    response, err := client.ShowRecycleBin(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](#).

5.20.3 Updating the Recycle Bin Policy

Function

This API is used to update the recycle bin policy. If recycle bin is not enabled, an error is reported.

Calling Method

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

URI

PUT /v3/{project_id}/elb/recycle-bin/policy

Table 5-797 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Request Parameters

Table 5-798 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Table 5-799 Request body parameters

Parameter	Mandatory	Type	Description
recycle_bin	No	RecycleBinPolicyRequestBody object	Definition: Request body for updating the recycle bin policy.

Table 5-800 RecycleBinPolicyRequestBody

Parameter	Mandatory	Type	Description
policy	No	RecycleBinPolicy object	Definition: Specifies the recycle bin policy.

Table 5-801 RecycleBinPolicy

Parameter	Mandatory	Type	Description
recycle_thresh old_hour	No	Integer	Definition: Specifies how old a deleted or unsubscribed load balancer has to be for it to be moved to the recycle bin. A load balancer can only be moved to the recycle bin if it has been there longer than the specified number of days in the policy. Range: N/A
retention_hour	No	Integer	Definition: Specifies how long you want your load balancers to be kept in the recycle bin. Range: N/A

Response Parameters

Status code: 200

Table 5-802 Response body parameters

Parameter	Type	Description
recycle_bin	RecycleBinResponseBody object	Definition: Specifies the response body for the recycle bin.

Table 5-803 RecycleBinResponseBody

Parameter	Type	Description
project_id	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Range: The value can contain a maximum of 32 characters, including digits and lowercase letters.
policy	RecycleBinPolicy object	Definition: Specifies the recycle bin policy.

Parameter	Type	Description
enable	Boolean	Definition: Specifies whether to enable recycle bin. Range: • true: Enable recycle bin. • false: Disable recycle bin.

Table 5-804 RecycleBinPolicy

Parameter	Type	Description
recycle_threshold_hour	Integer	Definition: Specifies how old a deleted or unsubscribed load balancer has to be for it to be moved to the recycle bin. A load balancer can only be moved to the recycle bin if it has been there longer than the specified number of days in the policy. Range: N/A
retention_hour	Integer	Definition: Specifies how long you want your load balancers to be kept in the recycle bin. Range: N/A

Example Requests

```
https://{ELB_Endpoint}/v3/7b7705dce1e847b08b3b16dda67fec24/elb/recycle-bin/policy

{
  "recycle_bin" : {
    "policy" : {
      "recycle_threshold_hour" : 21,
      "retention_hour" : 20
    }
  }
}
```

Example Responses

Status code: 200

Response body for updating the recycle bin policy

```
{
  "recycle_bin" : {
    "enable" : true,
    "policy" : {
      "recycle_threshold_hour" : 20,
      "retention_hour" : 20
    },
    "project_id" : "7b7705dce1e847b08b3b16dda67fec24"
```

```
}  
}
```

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 UpdateRecycleBinPolicySolution {  
  
    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();  
        UpdateRecycleBinPolicyRequest request = new UpdateRecycleBinPolicyRequest();  
        UpdateRecycleBinPolicyRequestBody body = new UpdateRecycleBinPolicyRequestBody();  
        RecycleBinPolicy policyRecycleBin = new RecycleBinPolicy();  
        policyRecycleBin.withRecycleThresholdHour(21)  
            .withRetentionHour(20);  
        RecycleBinPolicyRequestBody recycleBinbody = new RecycleBinPolicyRequestBody();  
        recycleBinbody.withPolicy(policyRecycleBin);  
        body.withRecycleBin(recycleBinbody);  
        request.withBody(body);  
        try {  
            UpdateRecycleBinPolicyResponse response = client.updateRecycleBinPolicy(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 = UpdateRecycleBinPolicyRequest()
        policyRecycleBin = RecycleBinPolicy(
            recycle_threshold_hour=21,
            retention_hour=20
        )
        recycleBinbody = RecycleBinPolicyRequestBody(
            policy=policyRecycleBin
        )
        request.body = UpdateRecycleBinPolicyRequestBody(
            recycle_bin=recycleBinbody
        )
        response = client.update_recycle_bin_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.ElClientBuilder().
        WithRegion(region.ValueOf("<YOUR REGION>")).
        WithCredential(auth).
        Build())

request := &model.UpdateRecycleBinPolicyRequest{
    recycleThresholdHourPolicy:= int32(21)
    retentionHourPolicy:= int32(20)
    policyRecycleBin := &model.RecycleBinPolicy{
        RecycleThresholdHour: &recycleThresholdHourPolicy,
        RetentionHour: &retentionHourPolicy,
    }
    recycleBinbody := &model.RecycleBinPolicyRequestBody{
        Policy: policyRecycleBin,
    }
    request.Body = &model.UpdateRecycleBinPolicyRequestBody{
        RecycleBin: recycleBinbody,
    }
    response, err := client.UpdateRecycleBinPolicy(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	Response body for updating the recycle bin policy

Error Codes

See [Error Codes](#).

5.20.4 Querying Load Balancers in the Recycle Bin

Function

This API is used to query load balancers in the recycle bin.

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/recycle-bin/loadbalancers

Table 5-805 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Table 5-806 Query Parameters

Parameter	Mandatory	Type	Description
marker	No	String	Definition: Specifies the ID of the last record on the previous page. Constraints: - This parameter must be used together with limit. - If the parameter is not specified, only resources on the first page are queried. - This parameter cannot be left blank or set to an invalid ID. Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
limit	No	Integer	Definition: Specifies the number of records returned on each page. Constraints: N/A Range: 0 to 2000 Default value: 2000
page_reverse	No	Boolean	Definition: Specifies whether to use reverse query. Constraints: • This parameter must be used together with limit. • If page_reverse is set to true and you want to query the resources on the previous page, set the value of marker to the value of previous_marker. Range: • true: Query resources on the previous page. • false: Query resources on the next page. Default value: false
id	No	Array of strings	Specifies the load balancer ID. Multiple IDs can be used for query in the format of <i>id=xxx&id=xxx</i> .
name	No	Array of strings	Specifies the load balancer name. Multiple names can be used for query in the format of <i>name=xxx&name=xxx</i> .
description	No	Array of strings	Provides supplementary information about the load balancer. Multiple descriptions can be used for query in the format of <i>description=xxx&description=xxx</i> .

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Definition: Specifies whether the load balancer is enabled. Range: • true: enabled • false: disabled
operating_status	No	Array of strings	Specifies the operating status of the load balancer. Value options: • ONLINE: The load balancer is working normally. • FROZEN: The load balancer has been frozen. Multiple operating statuses can be used for query in the format of <i>operating_status=xxx&operating_status=xxx</i> .
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.
vpc_id	No	Array of strings	Specifies the ID of the VPC where the load balancer resides. Multiple IDs can be used for query in the format of <i>vpc_id=xxx&vpc_id=xxx</i> .
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 used for query in the format of <i>vip_port_id=xxx&vip_port_id=xxx</i> .

Parameter	Mandatory	Type	Description
<code>vip_address</code>	No	Array of strings	Specifies the IPv4 private IP address of the load balancer. Multiple IP addresses can be used for query in the format of <i>vip_address=xxx&vip_address=xxx</i> .
<code>vip_subnet_cidr_id</code>	No	Array of strings	Specifies the ID of the IPv4 subnet where the load balancer resides. Multiple IDs can be used for query in the format of <i>vip_subnet_cidr_id=xxx&vip_subnet_cidr_id=xxx</i> .
<code>ipv6_vip_port_id</code>	No	Array of strings	Specifies the ID of the port bound to the IPv6 address of the load balancer. Multiple ports can be used for query in the format of <i>ipv6_vip_port_id=xxx&ipv6_vip_port_id=xxx</i> .
<code>ipv6_vip_address</code>	No	Array of strings	Specifies the IPv6 address bound to the load balancer. Multiple IPv6 addresses can be used for query in the format of <i>ipv6_vip_address=xxx&ipv6_vip_address=xxx</i> .
<code>ipv6_vip_virsubnet_id</code>	No	Array of strings	Specifies the ID of the IPv6 subnet where the load balancer resides. Multiple IDs can be used for query in the format of <i>ipv6_vip_virsubnet_id=xxx&ipv6_vip_virsubnet_id=xxx</i> .

Parameter	Mandatory	Type	Description
eips	No	Array of strings	Specifies the IPv4 EIP bound to the load balancer. The following is an example: <pre>"eips": [{ "eip_id": "e9b72a9d-4275-455e- a724-853504e4d9c6", "eip_address": "88.88.14.122", "ip_version": 4 }]</pre> Multiple EIPs can be used for query. • If eip_id is used as the query condition, the format is <i>eips=eip_id=xxx&eips=eip_id=xxx.</i> • If eip_address is used as the query condition, the format is <i>eips=eip_address=xxx&eips=eip_address=xxx.</i> • If ip_version is used as the query condition, the format is <i>eips=ip_version=xxx&eips=ip_version=xxx.</i> Note that this parameter has the same meaning as publicips.

Parameter	Mandatory	Type	Description
publicips	No	Array of strings	Specifies the EIP bound to the load balancer. The following is an example: <pre>"publicips=": [{ "public_id": "e9b72a9d-4275-455e- a724-853504e4d9c6", "public_address": "88.88.14.122", "ip_version": 4 }]</pre> If you want to query the load balancers that have the above EIP bound, you can use the following format: <pre>publicips=ip_version %3D4&publicips=public_addre ss %3D88.88.14.122&publicips=p ublic_id %3De9b72a9d-4275-455e- a724-853504e4d9c6</pre> Multiple values can be used for query in the format of: • If publicip_id is used as the query condition, the format is <i>publicips=publicip_id=xxx&publicips=publicip_id=xxx.</i> • If publicip_address is used as the query condition, the format is <i>publicips=publicip_address=xxx&publicips=publicip_address=xxx.</i> • If ip_version is used as the query condition, the format is <i>publicips=ip_version=xxx&publicips=ip_version=xxx.</i> Note: 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 used for query in the format of <i>availability_zone_list=xxx&availability_zone_list=xxx</i> .
l4_flavor_id	No	Array of strings	Specifies the ID of a flavor at Layer 4. Multiple IDs can be used for query in the format of <i>l4_flavor_id=xxx&l4_flavor_id=xxx</i> .
l7_flavor_id	No	Array of strings	Specifies the ID of a flavor at Layer 7. Multiple flavors can be used for query in the format of <i>l7_flavor_id=xxx&l7_flavor_id=xxx</i> .
billing_info	No	Array of strings	Provides resource billing information. Multiple values can be used for query in the format of <i>billing_info=xxx&billing_info=xxx</i> . This parameter is unsupported. Please do not use it.
member_device_id	No	Array of strings	Specifies the ID of the ECS 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 used for query in the format of <i>member_device_id=xxx&member_device_id=xxx</i> .

Parameter	Mandatory	Type	Description
member_address	No	Array of strings	Specifies the private IP address of the ECS 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 used for query in the format of <i>member_address=xxx&member_address=xxx</i>.
enterprise_project_id	No	Array of strings	Definition: Specifies the ID of the enterprise project where the load balancer is used. Multiple values can be used for query in the format of: <i>enterprise_project_id=xxx&enterprise_project_id=xxx</i>. Constraints: • 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. Range: N/A Default value: N/A

Parameter	Mandatory	Type	Description
ip_version	No	Array of integers	Specifies the IP version. The value can be 4 (IPv4) or 6 (IPv6). Multiple versions can be used for query in the format of <i>ip_version=xxx&ip_version=xxx</i> .
deletion_protection_enable	No	Boolean	Definition: Specifies whether to enable deletion protection. Constraints: N/A Range: false (disable this option) or true (enable this option). Default value: N/A
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 used for query in the format of <i>elb_virsubnet_type=ipv4&elb_virsubnet_type=dualstack</i> .
autoscaling	No	Array of strings	Specifies whether to enable elastic scaling. Example: "autoscaling": { "enable": "true" } Multiple values can be used for query in the format of <i>autoscaling=enable=true&autoscaling=enable=false</i> .
protection_status	No	Array of strings	Specifies the protection status. Value options: • nonProtection (default): The resource is not protected. • consoleProtection: Modification is not allowed 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: <pre>{ "global_eips": [{ "global_eip_id": "240000000-0000-0000-0000-1 000000000001", "global_eip_address": "10.10.10.10", "ip_version": 4 }] }</pre> Multiple values can be used for query in the format of: • If global_eip_id is used as the query condition, the format is <i>global_eips=global_eip_id=xxx&global_eips=global_eip_id=xxx.</i> • If global_eip_address is used as the query condition, the format is <i>global_eips=global_eip_address=xxx&global_eips=global_eip_address=xxx.</i> • If ip_version is used as the query condition, the format is <i>global_eips=ip_version=xxx&global_eips=ip_version=xxx.</i>
log_topic_id	No	String	Specifies the ID of the log topic that is associated with the load balancer. Multiple IDs can be used for query in the format of <i>log_topic_id=xxx&log_topic_id=xxx.</i>

Parameter	Mandatory	Type	Description
log_group_id	No	String	Specifies the ID of the log group that is associated with the load balancer. Multiple IDs can be used for query in the format of <i>log_group_id=xxx&log_group_id=xxx</i> .

Request Parameters

Table 5-807 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 5-808 Response body parameters

Parameter	Type	Description
loadbalancers	Array of RecycleLoadBalancer objects	Lists the load balancers in the recycle bin. Range: N/A
page_info	PageInfo object	Definition: Specifies the pagination information.
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).

Table 5-809 RecycleLoadBalancer

Parameter	Type	Description
id	String	Definition: Specifies the load balancer ID. Range: N/A

Parameter	Type	Description
auto_terminate_time	String	Specifies the time when the load balancers in the recycle bin will be permanently deleted, in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> . Range: N/A
description	String	Definition: Provides supplementary information about the load balancer. Range: N/A
provisioning_status	String	Definition: Specifies the provisioning status of the load balancer. Range: • RECYCLING: The load balancer is kept in the recycle bin.
admin_state_up	Boolean	Definition: Specifies whether the load balancer is enabled. Range: • true: enabled • false: disabled
provider	String	Definition: Specifies the provider of the load balancer. The value is fixed to vlb . Range: N/A
pools	Array of PoolRef objects	Definition: Lists the IDs of backend server groups associated with the load balancer.
listeners	Array of ListenerRef objects	Definition: Lists the IDs of listeners associated with the load balancer.
operating_status	String	Definition: Specifies the operating status of the load balancer. Range: • ONLINE: The load balancer is online. • FROZEN: The load balancer is frozen.
name	String	Definition: Specifies the load balancer name. Range: N/A

Parameter	Type	Description
project_id	String	Definition: Specifies the ID of the project where the load balancer is used. Range: N/A
vip_subnet_cidr_id	String	Definition: Specifies the ID of the IPv4 subnet where the load balancer is located. This subnet is also called the frontend subnet. Range: N/A
vip_address	String	Definition: Specifies the private IPv4 address of the load balancer. Range: N/A
vip_port_id	String	Definition: Specifies the ID of the port bound to the private IPv4 address of the load balancer. Range: N/A
tags	Array of Tag objects	Definition: Specifies the tags added to the load balancer.
created_at	String	Definition: Specifies the time when the load balancer was created. Range: The value must be in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> .
updated_at	String	Definition: Specifies the time when the load balancer was updated. Range: The value must be in the format of <i>yyyy-MM-dd'T'HH:mm:ss'Z'</i> .
guaranteed	Boolean	Definition: Specifies whether the load balancer is a dedicated load balancer. Range: • false: The load balancer is a shared load balancer. • true: The load balancer is a dedicated load balancer.
vpc_id	String	Definition: Specifies the ID of the VPC where the load balancer is located. Range: N/A

Parameter	Type	Description
eips	Array of EipInfo objects	Definition: Specifies the EIP bound to the load balancer. NOTE This parameter has the same meaning as publicips .
ipv6_vip_address	String	Definition: Specifies the IPv6 address of the load balancer. Range: N/A
ipv6_vip_virsubnet_id	String	Definition: Specifies the ID of the IPv6 subnet where the load balancer is located. This subnet is also called the frontend subnet. Range: N/A
ipv6_vip_port_id	String	Definition: Specifies the ID of the port bound to the IPv6 address of the load balancer. Range: N/A
availability_zone_list	Array of strings	Definition: Specifies the list of AZs where the load balancers are created. Range: N/A
enterprise_project_id	String	Definition: Specifies the ID of the enterprise project. Range: • 0: The resource belongs to the default enterprise project. • A string in UUID format indicates a non-default enterprise project.
billing_info	String	Definition: Provides resource billing information. Range: • If the value is left blank, the resource is billed on a pay-per-use basis.
l4_flavor_id	String	Definition: Specifies the ID of a flavor at Layer 4. For an instance with elastic flavor, this parameter defines the maximum elastic flavor at Layer 4. Range: N/A

Parameter	Type	Description
l4_scale_flavor_id	String	Definition: Specifies the ID of the elastic flavor at Layer 4. Range: N/A This parameter is unsupported. Please do not use it.
l7_flavor_id	String	Definition: Specifies the ID of a flavor at Layer 7. For an instance with elastic flavor, this parameter defines the ID of the maximum elastic flavor at Layer 7. Range: N/A
l7_scale_flavor_id	String	Definition: Specifies the ID of an elastic flavor at Layer 7. Range: N/A This parameter is unsupported. Please do not use it.
publicips	Array of PublicIpInfo objects	Definition: Specifies the EIP bound to the load balancer. Only one EIP can be bound to a load balancer. NOTE This parameter has the same meaning as eips .
global_eips	Array of GlobalEipInfo objects	Definition: Specifies the global EIP bound to the load balancer.
elb_virsubnet_ids	Array of strings	Definition: Specifies the network IDs of subnets on the downstream plane. Range: N/A
elb_virsubnet_type	String	Definition: Specifies the type of the subnet on the downstream plane. Range: • ipv4: IPv4 subnets • dualstack: subnets support IPv4/IPv6 dual stack

Parameter	Type	Description
ip_target_enable	Boolean	Definition: Specifies whether to add backend servers that are not in the load balancer's VPC. 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. Range: • true: This option will be enabled. • false: This option will be disabled.
frozen_scene	String	Definition: Specifies the scenario where the load balancer is frozen. If there are multiple scenarios, separate them with commas (,). Range: • 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. • AREAR: The load balancer is frozen due to arrears.
ipv6_bandwidth	BandwidthRef object	Definition: Specifies the ID of the bandwidth.
deletion_protection_enable	Boolean	Definition: Specifies whether to enable deletion protection. Range: • false: This option will be disabled. • true: This option will be enabled.

Parameter	Type	Description
autoscaling	AutoscalingRef object	Definition: Specifies information about elastic scaling. If elastic scaling is enabled, the load balancer flavors can be automatically adjusted based on incoming traffic. NOTE 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 flavors will be created and you will be billed for the minimum flavors.
public_border_group	String	Definition: Specifies the AZ group to which the load balancer belongs. Range: N/A
charge_mode	String	Definition: Specifies the charge mode of the load balancer. Range: • flavor: billed by the fixed flavor you select. • lcu: billed by how many LCUs you have used. • Null: If it is a shared load balancer, it is free. If it is a dedicated load balancer, it will be billed by the fixed flavor you select.
waf_failure_action	String	Definition: Specifies traffic distributing policies when the WAF is faulty. Range: discard indicates traffic will not be distributed. forward indicates traffic will be distributed to the default backend servers.
protection_status	String	Definition: Specifies the protection status. Constraints: N/A Range: • nonProtection (default): The resource is not protected. • consoleProtection: Modifications are not allowed on the console. Default value: N/A

Parameter	Type	Description
protection_reason	String	Definition: Specifies why modification protection is enabled. Range: The value can contain a maximum of 255 Unicode characters, excluding angle brackets (<>).
log_group_id	String	Definition: Specifies the ID of the log group that is associated with the load balancer. Range: N/A
log_topic_id	String	Definition: Specifies the ID of the log topic that is associated with the load balancer. Range: N/A

Table 5-810 PoolRef

Parameter	Type	Description
id	String	Definition: Specifies the backend server group ID. Range: N/A

Table 5-811 ListenerRef

Parameter	Type	Description
id	String	Definition: Specifies the listener ID. Range: N/A

Table 5-812 Tag

Parameter	Type	Description
key	String	Definition: Specifies the tag key. Range: N/A
value	String	Definition: Specifies the tag value. Range: N/A

Table 5-813 EipInfo

Parameter	Type	Description
eip_id	String	Definition: Specifies the EIP ID. Range: N/A
eip_address	String	Definition: Specifies the EIP. Range: N/A
ip_version	Integer	Definition: Specifies the IP address version. Range: • 4: IPv4 addresses • 6: IPv6 addresses

Table 5-814 PublicIpInfo

Parameter	Type	Description
publicip_id	String	Definition: Specifies the EIP ID. Range: N/A
publicip_address	String	Definition: Specifies the EIP. Range: N/A
ip_version	Integer	Definition: Specifies the IP address version. Range: • 4: IPv4 address • 6: IPv6 address

Table 5-815 GlobalEipInfo

Parameter	Type	Description
global_eip_id	String	Definition: Specifies the ID of the global EIP. Range: N/A
global_eip_addresses	String	Definition: Specifies the global EIP. Range: N/A

Parameter	Type	Description
ip_version	Integer	Definition: Specifies the IP address version. Range: • 4: IPv4 addresses • 6: IPv6 addresses

Table 5-816 BandwidthRef

Parameter	Type	Description
id	String	Definition: Specifies the ID of the shared bandwidth. Constraints: N/A Range: N/A Default value: N/A

Table 5-817 AutoscalingRef

Parameter	Type	Description
enable	Boolean	Definition: Specifies whether to enable elastic scaling for the load balancer. Range: • true: This option will be enabled. • false: This option will be disabled.
min_l7_flavor_id	String	Definition: Specifies the ID of the minimum elastic flavor at Layer 7. Range: N/A

Table 5-818 PageInfo

Parameter	Type	Description
previous_marker	String	Definition: Specifies the ID of the first record in the pagination query result. If page_reverse is set to true , this parameter is used together to query resources on the previous page. Range: N/A

Parameter	Type	Description
next_marker	String	Definition: Specifies the ID of the last record in the pagination query result. It is usually used to query resources on the next page. Range: N/A
current_count	Integer	Definition: Specifies the number of records returned on the current page. Range: N/A

Example Requests

Querying load balancers on each page

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

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": "RECYCLING",
    "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_virusubnet_id": "0b9e3c5e-3ec8-46b3-bab9-80b1450e59ee",
    "ipv6_vip_port_id": "5186bb47-24e5-4171-b795-62d22846db9b",
    "publicips": [ ],
    "elb_virusubnet_ids": [ "0b9e3c5e-3ec8-46b3-bab9-80b1450e59ee" ],
    "elb_virusubnet_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,
"auto_terminate_time" : "2021-07-26T03:18:37Z"
}, {
  "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" : "RECYCLING",
  "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,
  "auto_terminate_time" : "2021-07-26T03:18:37Z"
} ],
```

```
"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 ListRecycleBinLoadBalancersSolution {  
  
    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();  
        ListRecycleBinLoadBalancersRequest request = new ListRecycleBinLoadBalancersRequest();  
        try {  
            ListRecycleBinLoadBalancersResponse response = client.listRecycleBinLoadBalancers(request);  
            System.out.println(response.toString());  
        } catch (ConnectionException e) {  
            e.printStackTrace();  
        } catch (RequestTimeoutException e) {  
            e.printStackTrace();  
        } catch (ServiceResponseException e) {  
            e.printStackTrace();  
            System.out.println(e.getStatusCode());  
            System.out.println(e.getRequestId());  
            System.out.println(e.getErrorCode());  
            System.out.println(e.getErrorMsg());  
        }  
    }  
}
```

Python

```
# coding: utf-8
```

```
import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from 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 = ListRecycleBinLoadBalancersRequest()
        response = client.list_recycle_bin_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.ListRecycleBinLoadBalancersRequest{}
    response, err := client.ListRecycleBinLoadBalancers(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](#).

5.20.5 Restoring a Load Balancer from the Recycle Bin

Function

This API is used to restore a load balancer from the recycle bin.

Calling Method

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

URI

PUT /v3/{project_id}/elb/recycle-bin/loadbalancers/{loadbalancer_id}/recover

Table 5-819 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A

Parameter	Mandatory	Type	Description
loadbalancer_id	Yes	String	Definition: Specifies the load balancer ID. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-820 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 200

Table 5-821 Response body parameters

Parameter	Type	Description
request_id	String	Definition: Specifies the request ID. Range: The value is automatically generated, and can contain characters including digits, lowercase letters, and hyphens (-).
type	String	Definition: Specifies the load balancer type. Range: • v2: shared load balancers • v3: dedicated load balancers
job_id	String	Definition: Specifies the restoration task ID. Range: N/A

Example Requests

None

Example Responses

Status code: 200

Successful request.

```
{
  "request_id" : "841e0da7-5835-4130-9a47-01688f34a154",
  "job_id" : "062804a2-9e39-4dde-bd9b-271859ee312b",
  "type" : "v3"
}
```

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 RestoreLoadbalancerSolution {

    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();
        RestoreLoadbalancerRequest request = new RestoreLoadbalancerRequest();
        request.withLoadbalancerId("{loadbalancer_id}");
        try {
            RestoreLoadbalancerResponse response = client.restoreLoadbalancer(request);
            System.out.println(response.toString());
        } catch (ConnectionException e) {
            e.printStackTrace();
        } catch (RequestTimeoutException e) {
            e.printStackTrace();
        } catch (ServiceResponseException e) {
            e.printStackTrace();
        }
    }
}
```

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

Python

```
# coding: utf-8

import os
from huaweicloudsdkcore.auth.credentials import BasicCredentials
from 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 = RestoreLoadbalancerRequest()
        request.loadbalancer_id = "{loadbalancer_id}"
        response = client.restore_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

```
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.RestoreLoadbalancerRequest{}
request.LoadbalancerId = "{loadbalancer_id}"
response, err := client.RestoreLoadbalancer(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](#).

5.20.6 Permanently Deleting a Load Balancer from the Recycle Bin

Function

This API is used to permanently delete a load balancer from the recycle bin. After the deletion, the load balancer cannot be restored.

Constraints

You can only permanently delete load balancers from the recycle bin.

Calling Method

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

URI

DELETE /v3/{project_id}/elb/recycle-bin/loadbalancers/{loadbalancer_id}

Table 5-822 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Definition: Specifies the project ID. For details about how to obtain a project ID, see Obtaining a Project ID . Constraints: N/A Range: The value can contain a maximum of 32 characters, including digits and lowercase letters. Default value: N/A
loadbalancer_id	Yes	String	Definition: Specifies the load balancer ID. Constraints: N/A Range: N/A Default value: N/A

Request Parameters

Table 5-823 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Definition: Specifies the token used for IAM authentication. Constraints: N/A Range: N/A Default value: N/A

Response Parameters

Status code: 204

Successful request.

None

Example Requests

Permanently deleting a load balancer from the recycle bin

```
DELETE https://{ELB_Endpoint}/v3/060576782980d5762f9ec014dd2f1148/elb/recycle-bin/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 DeleteRecycleLoadBalancerSolution {

    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();
        DeleteRecycleLoadBalancerRequest request = new DeleteRecycleLoadBalancerRequest();
        request.withLoadbalancerId("{loadbalancer_id}");
        try {
            DeleteRecycleLoadBalancerResponse response = client.deleteRecycleLoadBalancer(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 = DeleteRecycleLoadBalancerRequest()
        request.loadbalancer_id = "{loadbalancer_id}"
        response = client.delete_recycle_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.DeleteRecycleLoadBalancerRequest{}
    request.LoadbalancerId = "{loadbalancer_id}"
```

```
response, err := client.DeleteRecycleLoadBalancer(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](#).

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
<code>vip_address</code>	No	String	Specifies the private IP address of the load balancer. This IP address must be the one in the subnet specified by <code>vip_subnet_id</code>. If this parameter is not specified, an IP address is automatically assigned to the load balancer from the subnet specified by <code>vip_subnet_id</code>. 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.
<code>admin_state_up</code>	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
<code>enterprise_project_id</code>	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.
<code>protection_statuses</code>	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
<code>vip_address</code>	String	Specifies the private IP address of the load balancer. The value contains a maximum of 64 characters.
<code>listeners</code>	Array of Listeners objects	Lists the IDs of listeners added to the load balancer. For details, see Table 6-6 .
<code>pools</code>	Array of Pools objects	Lists the IDs of backend server groups associated with the load balancer. For details, see Table 6-7 .
<code>operating_status</code>	String	Specifies the operating status of the load balancer. The value can be ONLINE or FROZEN .
<code>provisioning_status</code>	String	This parameter is reserved, and its value can only be ACTIVE . It specifies the provisioning status of the load balancer.
<code>admin_state_up</code>	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.
<code>tags</code>	Array	Lists load balancer tags.
<code>created_at</code>	String	Specifies the time when the load balancer was created. The UTC time is in <i>YYYY-MM-DDTHH:MM:SS</i> format. The value contains a maximum of 19 characters.
<code>updated_at</code>	String	Specifies the time when the load balancer was updated. The UTC time is in <i>YYYY-MM-DDTHH:MM:SS</i> 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 <i>YYYY-MM-DDTHH:MM:SS</i> 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 <i>YYYY-MM-DDTHH:MM:SS</i> 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 <i>YYYY-MM-DDTHH:MM:SS</i> 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 <i>YYYY-MM-DDTHH:MM:SS</i> 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"
    }
  },
  "id": "c54b3286-2349-4c5c-ade1-e6bb0b26ad18",
  "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 <i>YYYY-MM-DDTHH:MM:SS</i> 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 <i>YYYY-MM-DDTHH:MM:SS</i> 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	Mandator y	Type	Description
project_id	Yes	Strin g	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 Loadbalance rs 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: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:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:AES128-SHA:AES256-SHA

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 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.
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 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.
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	Mandator y	Type	Description
project_id	Yes	Strin g	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 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.
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.

Parameter	Type	Description
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](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 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.
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	Mandator y	Type	Description
project_id	Yes	Strin g	Specifies the project ID.
pool_id	Yes	Strin g	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	Mandator y	Type	Description
project_id	Yes	Strin g	Specifies the project ID.
pool_id	Yes	Strin g	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": "xxxxxxxx"
    },
    "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	Mandator y	Type	Description
project_id	Yes	Strin g	Specifies the project ID.
pool_id	Yes	Strin g	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 <code>/</code>. The value starts with a slash (<code>/</code>). This parameter takes effect only when the value of type is set to HTTP. An example value is <code>/test</code>. 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	Healthmonit or 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 <code>/</code>. The value starts with a slash (<code>/</code>). This parameter takes effect only when the value of type is set to HTTP. An example value is <code>/test</code>. 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	Mandator y	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	Healthmonit or 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	Mandator y	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	Healthmonit or 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	Man dator y	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 <code>_~!;@^-%#&\$.*+?,=!: \() [] {}</code>

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	Mandator y	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 <code>_~';@^-%#&\$.*+?,=!: \()[]{}</code>

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 <code>_~';@^-%#&\$.*+?,:!= \()[]{}</code>
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 <code>_~!;@^-%#&\$.*+?,= : \()[]{}</code>

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 <code>_~';@^-%#&\$.*+?,=!: \()[]{}</code>
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	Mandator y	Type	Description
project_id	Yes	Strin g	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 <code>_~';@^-%#&\$. *+?,=!: \()[]{}</code>
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	Mandator y	Type	Description
project_id	Yes	Strin g	Specifies the project ID.
l7policy_id	Yes	Strin g	Specifies the forwarding policy ID.
l7rule_id	Yes	Strin g	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 <code>_~';@^-%#&\$.*+?=: \()[]{} </code>

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 <code>_~';@^-%#&\$.*+?;=!: \()[]{}</code>

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	Mandator y	Type	Description
project_id	Yes	Strin g	Specifies the project ID.
whitelist_id	Yes	Strin g	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 <i>YYYY-MM-DDTHH:MM:SS</i> format.

Parameter	Type	Description
create_time	String	Specifies the time when the certificate was created. The UTC time is in <i>YYYY-MM-DDTHH:MM:SS</i> format.
update_time	String	Specifies the time when the certificate was updated. The UTC time is in <i>YYYY-MM-DDTHH:MM:SS</i> 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-----
    \nMIIEvglBADANBgkqhkiG9w0BAQEFAASCBAKgwggSkAgEAAoIBAQDQVAbOLe5xNf4M
    \n253Wn9vhdUzojetjv4J+B7kYwsMhRcgdcj8KCnX1nfzTvl2ksXITQ2o9BkpStnPe
    \ntB4s32ZiJRMlk+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM
    \nMD30gLh6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8lCq39buNplgDOWzEP5AzqXt
    \nCOFYn6RTH5SRug4hKNN7sT1eYMSlHu7wtEBDKVgrLjOCe/W2f8rLT1zEsoAW2Chl
    \nZAPYUBkl/0XuTWRg3CohPPcl+UtlRSfvLDeeQ460swjbgwS/RbJh3slwlCRLU08k
    \nEo04Z9H/AgMBAAECggEAEleaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/Hl
    \nfvcArftGgMaYWPSSNCJRMXB7tPwpQu19esjz4Z/cR2Je4fTLPrffGUSHFgZjv5OQB
    \nZVe4a5Hj1OcgYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr
    \nciu9YklNNEHu6uRJ5g/eGGX3KQynTvVlhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M
    \nEGpfYI6AdHlwFZcT/RNAxhP82lg2gUJSgAu66FFdJmWQXKbafKdP3zq4Up8a7Ale
    \nkrGpuPtfV1vWklg+bUfhgGaiAEYTpAUN9t2DVIiijgQKBgQDnYMMsaF0r557CM1CT
    \nXUqgCZo8MKeV2jf2drlxRRwRL33SksQbzAQ/qRLdT7GP3sCGqvkwWY2FPdFYf8kx
    \nGcCeZPcleZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSPH7JNF3Tm/JH/fbwjpp7dt
    \nJ7n8EzkRUNE6aIMHOFeych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr
```

```
\niWgTWHXPZxUQaYhpjXo6+IMl6DpExiDgBAkMzJGlvS7yQiYWU+wthAr9urbWYdGZ
\nlS6VjoTkF6r7VZolLXX0fbuXh6lm8K8lQRfBpJff56p9phMwaBpDNDrfpHB5utBU
\nxs40yldp6wKBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zf3bGSXU/jR4eB
\n1lVQhELG9CbKsDzKM71GyElmix/T7FnSHIWLho1qVo6AQyduNWnAQD15pr8KAd
\nXGXAZZ1FQcb3KYa+2fflERmazedOTwjYZ0tGqZnXkEeMdSLkmqlCRigWhGQKbGdAk
\n/735uP20KKqhNehZpC2dJei7OilgRhCS/dKASUXHSW4fptBnUxACYocdDxtY4Vha
\nfl7FPMdvGL8ioYbvlHFH+X0Xs9r1S8yeWnHoXMB6eXWmYKMJrAoveLa+2cFm1Agf
\n7nLhA4R4lqm9lpV6SKegDUK4fxp9pPyodZPqBLLAoGBAJkD4wHW54PwD4Ctfk9o
\njHjWB7pQLUYpTZO9dm+4fpCMn9Okf43AE2yAOaAP94GdzdDjKxfciXKcsYr9lluk
\nfaoXgJkR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BUlGKMWXzuEd
\n3fy+1rCUwzOp9LSjtYf4ege\n-----END PRIVATE KEY-----",
"certificate":
"-----BEGIN CERTIFICATE-----
\nMIIC4TCCAcmgAwIBAgICEREWdQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXID
\nnb21wYW55IENBMBA4XDTE4MDcwMjEzMU0N1oXDTQ1MTEyNzEzMU0N1owFDESMBAG
\n\nA1UEAwJbG9jYWxob3N0MIIlBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
\n\nOFQGi3ucTX+DNud1p/b4XVM6I3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5
\n\nU0NqPQZKUzr3rQeL9mYiUTJZPutYlFDDbB8CtGv+eyU9yYJslWx/Bm5kWNPh9
\n\n7B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/W7jaS
\n\nlAzlxd+QM6l7QjHwJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQyLYKy4zgnv1tn/K
\n\nny09cxLKAftgoZWQD2FAZJf9F7k1kYNwqlTz3CPILZUUn7yw3nkOOTLMI28IEvOWy
\n\nYd7CMJQKs1NPJBKNOCfR/wlDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29t
\n\nnhwQKUuVjhwr/AAABMBMGA1UdJQMMAoGCCsGAQUFBwMBMA0GCsGSIb3DQEBCwUA
\n\nA4IBAQA8lMQxaTey7EjXtRSLVIEAMftAQPG6ijjNQuvIBYQUDauDT4W2XU25wAn
\n\nnjiOyQ83va672K1G9s8n6xLH+xwwdSNnozaKzC87vwSeZKI0dI9I5I98TGKI6OoDa
\n\nnezmcwQYtHBMVQ4c7MI8554Ft1mWSt4dMAK2rzNyjvPRLYLzp1HMnl6hkjPk4PCZ
\n\nnwKnha0dlScati9Cct3UzXSNJOSLalKdHErH08lqd+1BchScxCfk0xNITn1HZZGml
\n\n+vbmunok3A2luc14rnsrbkGYqXGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZ
\n\niYsGDVN+9QBD0eYUHce+77s96i3l\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+B7kYwsMhRcgdcJ8KcN1nfzTvl2ksXLTQ2o9BkpStnP
\nB4s32ZiJRmlk+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM
\nMD30gLh6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8lCq39buNplgDOWzEP5AqZt
\nCOFYn6RTH5SRug4hKNN7sT1eYMsLHu7wtEBDKVgrLjOCe/W2f8rLT1zESLAW2Chl
\nZAPYUBkl/0XuTWVRg3CohPPcl+UtlRSfvLDeeQ460swjbgwS/RbJh3slwLCrU08k
\nEo04Z9H/AgMBAAECggEAEleaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/Hl
\nfvfCArftGgMaYWPSPNCJRMXB7tPwpQu19esjz4Z/cR2Je4fTLPrffGUsHFgZjv5OQB
\nZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr
\nnciu9YklnNEHu6uRj5g/eGGX3KQynTvVlhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M
\nEGpfYl6AdHlwFZCT/RNAXhP82lg2gUJSgAu66FFdJmWQXKbafKdP3zq4Up8a7Ale
\nnkrguPtfv1vWklg+bUfhGaiAEYTpAUN9t2DVliijgQKBgQDnYMMsaF0r557CM1CT
\nXUqgCZo8MKeV2jf2drLxRRwRL33SksQbzAQ/qRLd7GP3sCGqvkvWY2FPdFYf8kx
\nGcCeZPcleZYQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/fbwjppJ7dt
\nJ7n8EzkrUNE6alMHOFeeYch/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr
\nniWgTWHXPZxUQaYhpjXo6+IMl6DpExiDgBAkMzJGlvS7yQiYWU+wthAr9urbWYdGZ
\n\nlS6VjoTkF6r7VZolLXX0fbuXh6lm8K8lQRfBpJff56p9phMwaBpDNDrfpHB5utBU
\n\nxs40yldp6wKBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zf3bGSXU/jR4eB
\n\n1lVQhELG9CbKsDzKM71GyElmix/T7FnSHIWLho1qVo6AQyduNWnAQD15pr8KAd
\n\nXGXAZZ1FQcb3KYa+2fflERmazedOTwjYZ0tGqZnXkEeMdSLkmqlCRigWhGQKbGdAk
\n\n/735uP20KKqhNehZpC2dJei7OilgRhCS/dKASUXHSW4fptBnUxACYocdDxtY4Vha
\n\nfl7FPMdvGL8ioYbvlHFH+X0Xs9r1S8yeWnHoXMB6eXWmYKMJrAoveLa+2cFm1Agf
\n\n3fy+1rCUwzOp9LSjtYf4ege\n-----END PRIVATE KEY-----",
  "certificate": "-----BEGIN CERTIFICATE-----
\nMIIC4TCCAcmgAwIBAgICEREWdQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXID
\nnb21wYW55IENBMBA4XDTE4MDcwMjEzMU0N1oXDTQ1MTEyNzEzMU0N1owFDESMBAG
\n\nA1UEAwJbG9jYWxob3N0MIIlBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
\n\nOFQGi3ucTX+DNud1p/b4XVM6I3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5
\n\nU0NqPQZKUzr3rQeL9mYiUTJZPutYlFDDbB8CtGv+eyU9yYJslWx/Bm5kWNPh9
\n\n7B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/W7jaS
\n\nlAzlxd+QM6l7QjHwJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQyLYKy4zgnv1tn/K
\n\nny09cxLKAftgoZWQD2FAZJf9F7k1kYNwqlTz3CPILZUUn7yw3nkOOTLMI28IEvOWy
\n\nYd7CMJQKs1NPJBKNOCfR/wlDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29t
\n\nnhwQKUuVjhwr/AAABMBMGA1UdJQMMAoGCCsGAQUFBwMBMA0GCsGSIb3DQEBCwUA
\n\nA4IBAQA8lMQxaTey7EjXtRSLVIEAMftAQPG6ijjNQuvIBYQUDauDT4W2XU25wAn
\n\nnjiOyQ83va672K1G9s8n6xLH+xwwdSNnozaKzC87vwSeZKI0dI9I5I98TGKI6OoDa
\n\nnezmcwQYtHBMVQ4c7MI8554Ft1mWSt4dMAK2rzNyjvPRLYLzp1HMnl6hkjPk4PCZ
\n\nnwKnha0dlScati9Cct3UzXSNJOSLalKdHErH08lqd+1BchScxCfk0xNITn1HZZGml
\n\n+vbmunok3A2luc14rnsrbkGYqXGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZ
\n\niYsGDVN+9QBD0eYUHce+77s96i3l\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."
}
```

```
\n7nLhA4R4lqm9lpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAJkD4wHW54Pwd4Ctfk9o
\njHjWB7pQlUYpTZO9dm+4fpCMn9Okf43AE2yAOaAP94GdzdDjKxfciXKcsYr9Iluk
\nfaoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BUIGKMWXzuEd
\n3fy+1rCUwzOp9LSjtYf4ege
\n-----END PRIVATE KEY-----",
  "certificate": "-----BEGIN CERTIFICATE-----
\nMIIC4TCCAcmgAwIBAgICERewDQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXID
\nb21wYW55IENBMB4XDTE4MDcwMjEzMjU0N1oXDTE4MTExNzEzMjU0N1owFDESMBAG
\nA1UEAwWJbG9jYWxob3N0MIIlBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
\n0FQGzi3ucTX+DNud1p/b4XVM6l3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5
\nU0NqPQZKUrZz3rQeLN9mYiUTJZPutYlFDDbB8CtIgV+eyU9yYJslWx/Bm5kWNPh9
\n7B9Yu9pbp2u6zDA99IC4ekKD93KuzxLnLmSle4Y3dbYwk0LpMDL6lfCHKt/W7jaS
\nlIAzlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylyKy4zgnv1tn/K
\nny09cxLKAftgoZWQD2FAZJf9F7k1kYNwqlTz3CPILZUUn7yw3nkOOTLMI28IEv0Wy
\nnYd7CMJQkS1NPJBKNOGfR/wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29t
\nnhwQKuUvJhwr/AAABMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCsqGSIb3DQEBcWUA
\nA4IBAQA8lMQxaTey7EjXtRLSVIEAMftAQPG6jjNQuvIBQYUDauDT4W2XU5wAn
\nnjiOyQ83va672K1G9s8n6xlH+xwwdSNnozaKzC87vwSeZKIodl9I5I98TGKI6OoDa
\nnezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPRLYLzp1HMn16hkPk4PCZ
\nnwKnha0dlScati9Cct3UzXSNJOSLaKdHErH08lqd+1BchScxCfk0xNITn1HZZGml
\n+vbmunok3A2luc14rnsrbkGYqxGikySN6B2cRLBDK4Y3wChiW6NVYtVqcX5/mZ
\nniYsGDVN+9QBd0eYUHce+77s96i3l
\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 <i>YYYY-MM-DD HH:MM:SS</i> format.
update_time	No	String	Specifies the time when the certificate was updated. The UTC time is in <i>YYYY-MM-DD HH:MM:SS</i> 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 <i>YYYY-MM-DD HH:MM:SS</i> format.
create_time	String	Specifies the time when the certificate was created. The UTC time is in <i>YYYY-MM-DD HH:MM:SS</i> format.
update_time	String	Specifies the time when the certificate was updated. The UTC time is in <i>YYYY-MM-DD HH:MM:SS</i> 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-----
\nMIIC4TCCAcmgAwIBAgICEREWDAQYKozIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXID
\nb21wYW55IENBMBA4XDTE4MDcwMjEzMDU0N1oXDTQ1MTExNzEzMDU0N1owFDESMBAG
\nA1UEAwJbG9jYWxob3N0MIIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAn0FQGzi3ucTX
+DNud1p/
b4XVM6I3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5\nU0NqPQZKURzZ3rQeLN9mYiUTJZPutYIFDDb
B8CtIgV+eyU9yYJslWx/
Bm5kWNPh9\n7B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6fCHKt/W7jaS
\nlAzlxsD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQyLYKy4zgnv1tn/K
\ny09cxLKAFTgoZWQD2FAZJf9F7k1kYNwqITz3CPILZUUn7yw3nkOOtLMI28IEvOWy
\nYd7CMJQkS1NPJBKNOGfR/wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29t
\nhwhwQKuUvJhwr/AAABMBMGA1UdJQMMAoGCCsGAQUFBwMBMA0GCsGSIb3DQEBwUA
\nA4IBAQA8lMQJxaTey7EjXtRLSVIEAMftAQP6GijjNQuvIBQYUDauDT4W2XU5wAn
\nnjiOyQ83va672K1G9s8n6xIH+xwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDa
\nnezmcwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPRLYlzp1HMnl6hkjPk4PCZ
\nnwK nha0dlScati9CCt3UzXSNJOSLaKdHErH08lqd+1BchScxCfk0xNItn1HZZGml\n
+vbmunok3A2luc14rnsrbkGYqXGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZ\niYsGDVN
+9QBd0eYUHce+77s96i3l\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+B7kYwsMhRcgdcJ8KcN1nfzTvl2ksXITQ2o9BkpStnPe\ntB4s32ZiJRMlk
+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM
\nMD30gLh6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8lq39buNplgDOWzEP5AzaqXt
\nCOFYn6RTH5SRug4hKNN7sT1eYMsHu7wtEBDKVgrLjOCe/W2f8rLT1zEsoAW2Chl\nnZAPYUBkl/
0XuTWRg3CohPPcl+UtlRSfvLDDeeQ460swjbgwS/Rbjh3slwLCRLU08k\nnEo04Z9H/
AgMBAAECCgEAEleaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/Hl
\nfvfCARftGgMaYWPSPNCJRMXB7tPwpQu19esjz4Z/cR2Je4fTLPrffGUsHFgZjv5OQB
\nZVe4a5Hj1OcgYhwcQpS2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr
\nnciu9YklNNEHu6uRj5g/eGGX3KQynTvVlhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M\nnEGpfYI6AdHlWfZcT/
RNAxhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7Ale\nnkrgruPtfV1vWklg
+bUFhgGaiAEYTpAUN9t2DVIijgQKBgQDnYMMsaF0r557CM1CT
\nXUqgCZo8MKeV2jf2drLxRRwRL33SksQbzAQ/qrLdT7GP3sCGqvkvxWY2FPdFYf8kx
\nGcCeZPcleZYCQAM41pjtsaM8tVbLVWR8UtGBuQoPSph7JNF3Tm/JH/fbwjpp7dt
\nJ7n8EzKRUNE6aIMHOFEeych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr
\nniWgTWHXPZxUQaYhpjXo6+IMl6DpExiDgBAkMzJGlvS7yQIYyWU+wthAr9urbWYdGZ
\nlS6VjoTkF6r7VZolLXX0fBuXh6lm8K8lQRfBpjff56p9phMwaBpDNDrfpHB5utBU
\nnxs40yldp6wKBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zf3bGSXU/jR4eB
\nn1IVQhELGI9CbKSdzKM71GyElmix/T7FnJSHIWIho1qVo6AQyduNWnAQD15pr8KAd
\nXGXAZZ1FQcb3KYa+2fIERmazdOTwjY20tGqZnXkEeMdSLkmqlCRigWhGQKBgDak\nn/
735uP20KKqhNehZpC2dJei7OilgRhCS/dKASUXHSW4fptBnUxACYocdDxtY4Vha\nnfl7FPMdvGl8ioYbvlHFH
+X0Xs9r1S8yeWnHoXMB6eXWmYKMJrAoveLa+2cFm1Agf
\n7nLhA4R4lqm9lpV6SKegDUK4fxp9pPyodZPqBLLAoGBAJKD4wHW54PwD4Ctfk9o
\nHjWB7pQlUYpTZO9dm+4fpCMn9Okf43AE2yAOaAP94GdzdDJkxfciXKcsYr9Iluk
\nnfaoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BUIGKMWXzuEd\nn3fy
+1rCUwzOp9LSjtYf4ege\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-----
MIIFizCCBHOGAwIBAgIQBlQycV3bWsvScttv5rgRjANBgkqhkiG9w0BAQsFADBu
MQswCQYDVQQGEwJlVUzEVMBMBGGA1UEChMMRGRlbnUlnclnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNLcnQuY29tMS0wKwYDVQQDEYRFbmNyeXB0aW9uIEV2Z2XJ5d2hlcmlUg
RFYgVExTIENTBIC0gRzEwHhcNMTgwNzEwMDAwMDAwWhcNMTkwNzEwMTIwMDAwWjAU
MRlWEAYDVQDEwlpY2UxMjMudGswggEiMA0GCSCGSIb3DQEBAQUAA4IBDwAwggEK
AoBAQCCTDlQlMoAvylnR6X1dihhNwbdGesbMW6NWXZ7f7fp9XrB3KCqqbzL4Vmh9
PntvrpLJNeolgLqDZZc4zKbUkmqxy1dvGDs41coKzdtc9Ig23GVK48wfesnk5r50
afyU52R1JISHDOhiDhHOSyhrOzc2GreLrByWKfUaAue6rTnyMbZQaSPtrTAqsURZ
wcmJ6R3A6JwokOgxXBSu41ufPQIFkMgxygKxEBLzLJlRqCXQHfYoxbsTyolb6bjwp
w4H6vrcRIeCFags98APWoeKjy7eOP3UUm05F+OkOvXhrLxEqLPm/rlwE0PmVlmm9
DgBaFYb3xT/MTt2VRSfCJQHGlcslAgMBAAGjgg9JMIIcTaFbBgNVHSMEDGawBRV
dE+yck/1YlpQ0dfmUVyaAYca1zAdBgNVHQ4EFggQUEFavYXBNbIHbcbhaKcUKad+
qCEwlwYDVR0RBbwwGolJaWNIMTlzlNrrgg13d3cuaWNIMTlzlNrrMA4GA1UdDwEB
/wQEAwIFoDAdBgNVHSUEFjAUBGgrBgEFBQcDAQYIKwYBBQUHAWAwTAYDVR0gBEUw
QzA3BglghkgBhvh1sAQIwKjAoBggrBgEFBQcCARYcaHR0cHM6Ly93d3cuZGlnaWNL
cnQuY29tL0N0Y29lAgBgzngQwBAGewgYEGCCSGAQUFBwEBBHUwczAlBggrBgEFBQcw
AYYZaHR0cDovL29jc3AyLmRpZ2ljZXJ0LmNvbTBKbGgrBgEFBQcwoAoY+aHR0cDov
L2NhY2VydHMuzGlnaWNLcnQuY29tL0V0VzY3JS5CHRpB25FdmVyeXdoZXJlRFZUTFND
QS1HMS5jcncwYQYDVDR0TBAlwADCCAQGCisGAQQB1nkCBAIEGfUwEgfiA8AB2AKS5
CZC0GFgUgh7sTosxncAo8NZgE+RvfuvON3zQ7IDdwQAAABZlOnLCAIAAAQDAEwRQlh
AIx6gCXNqgmPdFofDfZtPzLYr64TTrR/+b9QKKHyl2EjBAIAWgu3BG2QK9tWqXpUN
lFadc0nvqmdovabg5nmRMan2mQB2Ald1v+zDfPiMQ5lfvNu/1aNR1Y2/0q1YMG0
6v9eolMPAAABZlOnLQEAQAQDAEwRQlhAIJvRe/7n88dD6KdhNrd4LdFjGARQNmta
Y/K2dFDOXPSfAiBoLRVWw8unHOL25RWHJU7Ost3XkNhQYtrLDJrnzo/9kZzANBgkq
hkiG9w0BAQsFAAOCAQEAgEqtX9cHmj4OnNA0iOGmf3nKS/u/UgGSY4EJfXwQp2bTZ
PCKqx0QA6HEAX59v+UilTojrNDi0WskRm/8SKBHTmRWzW3Xile8KiR6ffKqPulVt
XHZcTfAFo47c7axqon8vumMLEv1PxVlmivQ446K7z3kGm34dhMYxS4G2g2tLI8Kt
90OegejuhbA55Wlvp1BK8HlYl5+mw+cgkUC9KTAL5sqVbWz0gb0S20KaYarGcu
otcZAOMeJdBFWnpzhr1fxmjaNY4u4hrgPZSTU/iBjdHapoza3zAffxysmGYqs9dR
fJyxZeR4scz8GqSTFviNdH9jvtDjKdAC5hfMaB811Q==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEqjCCA5KgAwIBAgIQAnmsRYVbsKwR+YBTzSybsTANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJlVUzEVMBMBGGA1UEChMMRGRlbnUlnclnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNLcnQuY29tMSAwHgyDVQQDEXdEaWdpQ2VydCBHbG9iYWwWgUm9vdCtB
QTAeFw0xNzExMjMxMjM1MjBwF0YnZExMjMxMjQ2MTBMAzG4c3RlbnVAYTA1VDT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydCj5
b20xLTArBgNVBAMTJEVUy3J55CHRpB24gRXZlcnJlbnN3ZSBEVIBUTFMgQOEglSBH
MTCCASlwdQYJKoZIhvcNAQEBBQADggEPADCCAQcCggEBALPeP6wkab41dyQh6mKc
oHqt3JrlXw5MDvf9Qyior7VfFwk665es0UFIb74N9pRntzF1UgYzRdp3ppZVMdo
lbxhm6dWS9OKl/iFehKNt0OYl9aqk6F+U7CA6jxSC+idBPXwdF4rs3KRGyp3aQnpj
pp1yr7lB6Y4zv72Ee/PLZ/6rk6InC6WpK0nPOVOR7n9iDuPe1E4lxUMBH/T33+3h
yuH3dvfgjWUOUkjdpmByxX+XNle5uEliYBsi4lvbctCh8ruifClI5mDXkZrmtM8n
wFYCV6v6kDdXkbgGRLKsR4pucbjtBkqlUGXuZl2t7pfewKRC5nWecvDBZf3+p1M
pA8CAwEAACAOWA8wggFLA1UdGgQWBBRvE+yck/1YlpQ0dfmUVyaAYca1zAf
BgNVHSMEDGawBQBD31BtVtGMA2ubwo+1lg8OSvJ3RVTAQBgNVH48EBAMCAYYw
HQYDVR0lBBYwFAYIKwYBBQUHAWEGCCSGAQUFBwMCMBIGA1UdEwEB/wQIMAYBAf8C
AQAwNAYIKwYBBQUHAQEKEKdAmMCQGCGCCSGAQUFBzABhhhodHRwOi8vb2Nzc5kaWdp
Y2VydCj5b20wQgYDVR0fBDswOTA3oDWgM4YxaHR0cDovL2NybDMuzGlnaWNLcnQu
Y29tL0RpZ2lDZXJ0xvYmFsUm9vdENBLmNybDBMBG9NVHSAERTBDMDcGCWCGSGAGG
/WwBAjAQDAEwGCGCCSGAQUFBwIBFhXodHRwczovL3d3dy5kaWdpY2VydCj5b20vQ1BT
MAgGBmeBDAECAATANBgkqhkiG9w0BAQsFAAOCAQEAK3Gp6/aGq7aBZsxf/oQ+TD/B
SwW3AU4ETK+GQf2kFzYZkby55FfHdPomunx2HBzViUchGoofGgg7gHW0W3MIQAXW
M0r5LUyStcr82QDWWYNPaUy4taCQmyaJ+Vb+6wxHvZtSigOISNF2a6vg4rgexieiv
4YSB03Yqp2t3tZeZHM9ESfusk74nQyW7pRGezj+TC443CagCQOzzNmEXAP2SnCrJ
sNE2DpRVMmLBj6xBrdimOsC3N6cQuKwRkxzbVYjYjCAAA8T1L0l+9wXerLPvErj

```

```
rMKWaBFLmfK/AHNF4ZihwPGOc7w6UHczBZXH5RFzJNnww+WnKuTPI0HfnVH8lg==
-----END CERTIFICATE-----",
    "type": "server",
    "create_time": "2019-03-03 16:32:30",
    "private_key": "-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAUw5UDKAL8ij0el9XYoYtcG3RnrGzFujWV+336Y/V6wdyggq
pccyOFZh/T57b66SyTXqJYC6g2WXOMym1JJqsWNXbxg7ONXKCs3bXPSIntxLSuPM
H3rJ5Oa+dGn8LOdkdSZUhwzoYg4Rzksoazs3Nhq3i6wclihVGgLnuaq058jG80Gkj
7a0wKrFEWcHJiekdwOicKJDoMVwUruNbnz0lhZDIMcoCsRAS8yCS40agL0B2KMW7
E8qJW+o8KcOB+r3ESBHBQILPFAKVkaBCo8u3jj91FJtORfjPDr14a5cRKiD5v65c
BND5IZZpvQ4AWn2G98U/zLU9LUUnwiUB4CHLHQIDAQABAoIBAGs5rISompP2OwA8
virwVRVXdPUQ5oxvbuTPys+A59RxVIU8kFW+qJ4fJMYsOFrXLtOtq+5tK20YBru
1ZLVfVqAowrELXB/J2ID+WTMkLORLsNlq1kW+nC9LL6PDY98LLW/n7FoFSkGI5HT
AxFGNGUvpr2vlojuL6nGfmcM47uscJ9aP6lJxr4p70dhPVjZBdnMnXYwRkB3dZt/
E0B/p8J5i3oo5Rucv4DOFB+01wXGAVyx5/zce+NZdhyrivkj3hHV55SxGhVWzWhj
a3dAlbpKwYgflJj0inRdJYmljBdbGb2HFix7+ncBg8B2oerJXC6/fANwRGU5/LZU
5xuPVWkCgYEA6an8TY1unlGLYL5aBJ16Tx4usqMyTXr/T4zkQyftRPMt+ZuxVQHl
GHsg7XvLFNd04MBZxtKZAyVcpOm7OUYcl0i9ZAKWXXoXcBt1Oom3gz/7RjAUnp
k+myvxCUSQ2JSz4u3QBtyPVyYnyBFXrKqdKfcYyG85+yQVHBNMvrdvMCgYEAvd0C
hFmp83ha+VQp+9XN1DYZNUyqhibj/E3X9jAn+gDbzKxw/D9en2RlQYUrl8+il8
QKk4cfOxJYStQfxptz8QBPVeLajDN67zJ0Rk8AB50HHHCNSU8uFkaO8KxsvVjbLS
+JltqfJAeraXlinbp1Fxcg9DsQdMd6cw2DmrWa8CgYEA1UjIOUzo80i4HYWDC4Vn
OEK3o22do+WqmEVlsfG9BH5HEdGve7V3EO/6aY+1/ZXBDPvH8mRAs9v8lbeXow7
hWCIVZfB5jre8HyOU4l8dPUCmdxhJrL913rRluASSqBlet3ZztuXCNWzp1X4nBj
/yF3UqFQKZ7SiHCDAZVWo4sCgYEAj7al/BcNzIcynX2mldhdh583b4/Ll+YCNm2Z
5eDHscZKmx8fLcJRpZE8dXagPqXmwtj6E1vDvQWP9m06VDNctHfHB+nO0tLmidSk
evmbScuiaTRmmbJf2IThY0hlqNsc7PgKF2DTklstEr0hLDFE8Z6FN6f0PIdfMcbD
Ax6L5EMCgYEA0+qhuQftKqKqGdbXX9r3H8N0TVh27ByfL3kKVYy0dUJMvsOAq6d97
8mEhYhrYt88f1sFsPM7G09XpCcBXwiKxw8+CDt9auD4r1snBnlLpqMPmanf4UDXH
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-----
MIIDpTCCAo2gAwIBAgIJAKdmMObYnFvoMA0GCSqGSIb3DQEBCwUAMGkxZCZAJBgNV
BAYTAh4MQswCQYDVQQLIDAJ4eDELMAkGA1UEBwwCeHgxZCZAJBgNVBAMoMAnh4MQsw
CQYDVQQLIDAJ4eDELMAkGA1UEAwwCeHgxGTAXBgkqhkiG9w0BCQEWCnh4QDE2My5j
b20wHhcNMTCxMjA0MDM0MjQ5WhcNMjA0MjA0MDM0MjQ5WjBpMQswCQYDVQQLIDAJ4eDELMAkGA1UE
CwwCeHgxZCZAJBgNVBAMoMAnh4MRkwFwYJKoZIhvcNAQkBFgpp4eEAXNjMuY29tMIIIB
lJANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCGKCAQEAwZ5UJULajW7p6FVwGRQRjFN
2s8tZ/6LC3X82fajpVsYqF1xqEuUDndDXVD09E4u83MS6HO6a3bIVQDp6/klnYld
iE6Vp8HH5BSKaCWKVg8lGWg1UM9wZFnlyi14KgmpIFmCu9nA8yV/6MZAe6RSDmb
3iyNBmiZ8aZhGw2pl1YwR+15MVqFFGB+7ExkziROi7L8CFCyCezK2/oOOvQsH1dz
Q8z1JXWdg8/9Zx7Ktvgwu5PQM3cJtSHX6iBPokMU8Z8TugLITqQXKZOEGwajwvQ5
mf2DPKvgM08XAgALJcLigwD513koAdtUd5v+9irw+5LAuO3JclqwTvwY7/YwwID
AQABO1AwTjAdBgNVHQ4EFgQUo5A2tlu+bcUfvGTD7wmEkHXKfjcwHwYDVR0JBgww
FoAUo5A2tlu+bcUfvGTD7wmEkHXKfjcwDAYDVR0TBAAUwAwEB/zANBgkqhkiG9w0B
AQsFAAOCAQEAJW2rS6Mvlqk3GfEpboezx2J3X71z8Sxoqg6ntwB+rezvK3mc9H0
83qcVeUcoH+0A0ISHyFN4FvRQL6X1hEheHarYwJK4agb231vb5erasuGO463eYEG
r45fTuOm7SylV2xxbaBKrXJtpBp4WLL/s+LF+nklKjaOxkmxUX0sM4CTA7uFljpy
c8Tdr8lDDNqoUtMD8BrUCJi+7lmMXRcC3Qi3oZJW76ja+kZA5mKVFPd1ATih8TbA
i34R7EQDtFeiSvBdeKRsp8c0KT8H1B4IXNkkCQs2WX5p4lm99+ZtLD4glw8x6lc
i1YhgnQbn5E0hz55OLu5jvOkKQjPCW+8Kg==
-----END CERTIFICATE-----",
    "type": "server",
```

```
    "create_time": "2018-09-28 03:00:47",
    "private_key": "-----BEGIN RSA PRIVATE KEY-----
MIIeowIBAAKCAQEAwZ5UJULAJWr7p6FVwGRQRjFN2s8tZ/6LC3X82fajpVsYqF1x
qEuUDndDXVD09E4u83MS6HO6a3bIVQDp6/klnYldiE6Vp8HH5BSKaCWKVg8lGWg1
UM9wZFnlryi14KgmpIpmcu9nA8yV/6MZAe6RSDmb3iyNBmiZ8aZhGw2p11YwR+15
MVqFFGB+7ExkziROI7L8CFCyCezK2/oOOvQsH1dzQ8z1JXWdg8/9Zx7Ktvgwu5PQ
M3cJtSHX6iBPOkMU8Z8TugLLtQqXKZOEgwajwvQ5mf2DPkVgM08XAgALJcLigwD5
13koAdtJd5v+9irw+5LAuO3JclqwTvwy7u/YwwIDAQABAolBACU9S5fjD9/jTMXA
DRs08A+gGgZUxLn0xk+NAPX3LyB1tfdkCaFB8BccLzO6h3KZuwQOBPv6jkdVEDbx
Nwyw3eA/9GJslvKiHcOrejdvPyMaw9I8MA7NbXHajrY7KpqDQyk6sx+aUTcy5jg
iMXLWdwXYHhJ/1HVOo603oZyiS6HZeYU089NDUcX+1Sji3e5Ke0gPVXEgCq1O11/
rh24bMxnnwZo4PKBWdcMBN5Zf/4ij9vrZE+ffzW7vGBO48A5lvZxWU2U5t/OZQRtN
1uLOHmMFa0FIF2aWbTVfwdUWAFsvAOKHj9Vv8BXOUwKOUuEktdkfAlvrmsFrO/H
yDeYYPkCgYEA/S55CBbR0sMXpSZ56uRn8JHApZJhgkgvYr+FqDUq/e92nAzf01P
RoEBUajwrnf1ycevN/SDfhtWzq2XJGqhWdJmtpO16b7KBsC6BdRcH6dnOYh31jgA
vABMIP3wzI4zSVTyxRE8LDuboytF1mSCeV5tHYPQTZNwrplDnLQhywcGgYEAw8Yc
Uk/eiFr3hfH/ZohMfV5p82Qp7DNIGRzw8YtVG/3+vNXrAXW1VhugNhQY6L+zLtJC
aKn84ooup0m3YCg0hviNqIuvzfsuzQgtjTXyaE0cEwsjUusOmiuj09vVx/3U7siK
Hdj2d1CPCvQ6Q8tdi8jV320gMs05AtaBkZdsiWUCgYEA/Lw4Kk4f+xTKDFsrLUNf
75wcqhWVBiwBp7yQ7UX4EYsJPKZcHMRTk0EEcAbpyaJZE3i44vjp5ReXIHNLMfPs
uvi34J4Rfot0LN3n7cFrAi2+wpNo+MOBwrNzpRmijGP2uKKRq4JiMjFbKV/6utGF
Up7VxfwS904JYpqGaZctilECgYA1A6nZtF0riY6ry/uAdXpZHL8ONNqRZtWoT0kD
79otSVu5iSiRbaGcXsDExC52oKrSDAgFtbqQUiEOFG09UcXfoR6HwRkba2CiDwve
yHQLQI5Qrdxz8Mk0glrNrSM4FamcW9vi9z4kCbQyoC5C+4gqeUURpDlkQBWP2Y4
2ct/bQKBgHv8qCsQTZphOxc31BJPa2xVhuv18cEU3XLURVfUZ/1f43JhLp7gynS2
ep++LKUi9D0VGXY8bqvfljbeCoCeu85vl8NpCXwe/LoVoln+7KaVIZMwqoGMfgNL
nEqm7HWkNxHhf8A6En/ljleuddS1sf9e/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	Mandator y	Type	Description
project_id	Yes	Strin g	Specifies the project ID.
certificate_id	Yes	Strin g	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_u p	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 <i>YYYY-MM-DDTHH:MM:SS</i> format.
create_time	String	Specifies the time when the certificate was created. The UTC time is in <i>YYYY-MM-DDTHH:MM:SS</i> format.
update_time	String	Specifies the time when the certificate was updated. The UTC time is in <i>YYYY-MM-DDTHH:MM:SS</i> 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-----
    \nMIIC4TCCAcmgAwIBAgICEREWDAQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXID
    \nb21wYW55IENBMBA4XDTE4MDcwMjEzMDU0N1oXDTQ1MTEwNzEzMDU0N1owFDESMBAG
    \nA1UEAwwJbG9jYWxob3N0MIIlBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
    \n0FQGzi3ucTX+DNud1p/b4XVM6I3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5
    \nU0NqPQZKUrZz3rQeLN9mYiUTJZPutYlFDDbB8CtIgV+eyU9yYJslWx/Bm5kWNPh9
    \n7B9Yu9pbp2u6zDA99IC4ekKD93KuzxLnLmSle4Y3dbYwk0LpMDL6lfCHKt/W7jaS
    \nIaZlsx+QM6L7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQyLYKy4zgnv1tn/K
    \ny09cxLKAftgoZWQD2FAZJf9F7k1kYNwqlTz3CPILZUUn7yw3nkOOTLMI28IEv0WY
    \nyd7CMJQKs1NPJBKNOGfR/wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29t
    \nhwQKUuVjhwr/AAABMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCsGSIb3DQEBCwUA
    \nA4IBAQA8lMQxaTey7EjXtRLSVIEAMftAQPG6jjjNQuvIBQYUDauDT4W2XUZ5wAn
    \njiOyQ83va672K1G9s8n6xLH+xwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDa
    \nezmzCwQYtHBMVQ4c7MI8554Ft1mWSt4dMAK2rzNjYjvPRLYLzp1HMnl6hjkPk4PCZ
    \nnwKnha0dlScati9Cct3UzXSNJOSLalKdHErH08lqd+1BchScxCfk0xNITn1HZZGml
    \n+vbmunok3A2luc14rnsrbcKGyqGikySN6B2cRLBDK4Y3wChiW6NVYtVqcX5/mZ
    \niYsGDVN+9QBd0eYUHce+77s96i3l
    \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+B7kYwsMhRcgdcj8KCnX1nfzTvl2ksXLTQ2o9BkpStnP
      \ntB4s32ZiJRmlk+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM
      \nMD30gH6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8lCq39buNplgDOWzEP5AazXt
      \nCOFYn6RTH5SRug4hKNN7sT1eYMSlHu7wtEBDKVgrLjOCe/W2f8rLT1zEsoAW2Chl
      \nZAPYUBkl/0XuTWRg3CohPPcl+UtlRSfvLDeeQ460swjbgwS/RbJh3slwCRLU08k
      \nEo04Z9H/AgMBAAECggEAEleaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/Hl
      \nfvfCArftGgMaYWPSPNCJRMXB7tPwpQu19esjz4Z/cR2Je4fTLPrffGUSHFgZjv5OQB
      \n2V4a5Hj1OcgYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr
      \nciu9YklNNEHu6uRJ5g/eGGX3KQynTvlhNOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M
      \nEGpfYl6AdHlwFzCT/RNAXhP82lg2gUJSgAu66FFdJmWQXKbafKdP3zq4Up8a7Ale
      \nkrgruPtFv1vWklg+bUFhgGaiAEYTpAUN9t2DVLiijgQKBgQDnYMMsaF0r557CM1CT
      \nXUqgCZo8MKev2jf2drLRRwRL33SksQbzAQ/qRLd7GP3sCGqvkwY2FPdFyf8kx
      \nGcCeZPcleZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSP7JNF3Tm/JH/fbwjP7dt
      \nJ7n8EzkRUNE6alMHOFEEych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr
      \nniWgTWHXPZxUQaYhpjXo6+IMl6DpExiDgBAkMzJGlvS7yQiYWU+wthAr9urbWYdGZ
      \nLS6VjoTkF6r7VZolLXX0fbuXh6lm8K8lQRfBpJff56p9phMwaBpDNDrfpHB5utBU
      \nxs40Yldp6wKBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zf3bGSXU/jR4eB
      \nn1lVQhELGI9CbKSdzKM71GyElmix/T7FnSHIWLho1qVo6AQyduNWNnAQD15pr8KAd
      \nXGXAZZ1FQcb3KYa+2fLErmazdOTWjYz0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak
      \n/735uP20KKqhNehZpC2dJei7OilgRhCS/dKASUXHSW4fptBnUxACYocdDxtY4Vha
      \nfl7FPMdvGl8ioYbvlHFh+X0Xs9r1S8yeWnHoXMB6eXWmYKMrAoveLa+2cFm1Agf
      \n7nLhA4R4lqm9lpV6SKegDUK4fxp9pPyodZPqBLLAoGBAJKD4wHW54PwD4Ctfk9o
      \njHjWB7pQlUYpTZO9dm+4fpCMn9Okf43AE2yAOaAP94GdzdDJkxfciXKcsYr9lIuk
      \nfaoXgjkR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BUIGKMWXzuEd
      \n3fy+1rCUwzOp9LSjtYf4ege
      \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	Mandator y	Type	Description
project_id	Yes	Strin g	Specifies the project ID.
certificate_id	Yes	Strin g	Specifies the certificate ID.

Request

Table 6-218 Parameter description

Parameter	Mand atory	Type	Description
admin_state_u p	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 <i>YYYY-MM-DDTHH:MM:SS</i> format.
create_time	String	Specifies the time when the certificate was created. The UTC time is in <i>YYYY-MM-DDTHH:MM:SS</i> format.
update_time	String	Specifies the time when the certificate was updated. The UTC time is in <i>YYYY-MM-DDTHH:MM:SS</i> 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-----
    \nMIIC4TCCAcmgAwIBAgICEREWDAQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXID
    \nb21wYW55IENBM4XDTE4MDcwMjEzMjU0N1oXDTQ1MTExNzEzMjU0N1owFDESMBAG
    \nA1UEAwWJbG9jYWxob3N0MIIlBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
    \n0FQGzi3ucTX+DNud1p/b4XVM6I3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5
    \nU0NqPQZKUrZz3rQeLN9mYiUTJZPutYlFDDbB8CtIgV+eyU9yYJstWx/Bm5kWNPh9
    \n7B9Yu9pbp2u6zDA99IC4ekKD93KuzxLnLmSle4Y3dbYwk0LpMDL6lfCHKt/W7jaS
    \nIAzlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQyLYKy4zgnv1tn/K
    \ny09cxLKAftgoZWQD2FAZJf9F7k1kYNwqITz3CPILZUUn7yw3nkOOtLMI28IEv0Wy
    \nYd7CMJQkS1NPJBKNOGfR/wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29t
    \nnhwQKuUvJhWR/AAABMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCsGQSIb3DQEBCwUA
    \nA4IBAQA8IMQJxaTey7EjXtRLSVIEAMftAQPG6jijNQuvIBQYUDauDT4W2XU5wAn
    \nnjiOyQ83va672K1G9s8n6xlH+xwwdSNnozaKzC87vwSeZKI0dI9I5I98TGKI6OoDa
    \nezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNjvPRLYLzp1HMnl6hkjPk4PCZ
    \nnwKnh0dlScati9CCt3UzXSNJOSLaKdHErH08lqd+1BchScxChk0xNITn1HZZGml
    \n+vbmunok3A2luc14rnsrbcGyqxGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZ
    \nniYsGDVN+9QBd0eYUHce+77s96i3l
    \n-----END CERTIFICATE-----",
    "description": "description for certificate",
    "domain": "www.elb.com",
    "name": "https_certificate",
    "private_key":
      "-----BEGIN PRIVATE KEY-----
      \nMIIIEvglBADANBgkqhkiG9w0BAQEFAASCBKggwggSkAgEAAoIBAQQDQVAbOLe5xNf4M
      \n253Wn9vhdUzojetjv4J+B7kYwsMhRcgdcJ8KCnX1nfzTvI2ksXITQ2o9BkpStnPe
      \nbtB4s32ZiJRMlk+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM
      \nMD30gLf6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8lcq39buNpIgDOWzEP5AzqXt
      \nnciu9YklNNEHu6uRJ5g/eGGX3KQynTvVIhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M
      \nEGpfYI6AdHIwFZcT/RNAXhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7Ale
      \nkrgruPtFv1vWklg+bUfhGaiAEYTpAUN9t2DVliijgQKBgQDnYMMsaF0r557CM1CT
      \nXUqgCZ08MKev2jf2drLxRRwRL33SksQbzAQ/qrLdT7GP3sCGqvkvxWY2FPdFy8kx
      \nGcCeZPcleZYQCAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/fbwjpiP7dt
      \nn7n8EzkRUNE6alMHOFEeych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4LaR
      \nniWgTWHXPZuXQaYhpjXo6+IMl6DpExiDgBAkMzJGlvS7yQiYWU+wthAr9urbWYdGZ
```



```
\nIS6VjoTkF6r7VZoILXX0fbuXh6lm8K8lQRfBpJff56p9phMwaBpDNDrfpHB5utBU
\nxs40yldp6wKBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zf3bGSXU/jR4eB
\n1lVQhELGI9CbKSdzKM71GyElmix/T7FnSHIWLho1qVo6AQyduNWnAQD15pr8KAd
\nXGXAZZ1FQcb3KYa+2fflERmazdOTWjYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak
\n/735uP20KKqhNehZpC2dJei7OilgRhCS/dKASUXHSW4fptBnUxACYocdDxtY4Vha
\nfl7FPMdvGl8ioYbvlHFh+X0Xs9r1S8yeWnHoXMB6eXWmYKMrAoveLa+2cFm1Agf
\n7nLhA4R4lqm9lpV6SKegDUK4fxp9pPyodZPqBLLAoGBAJkD4wHW54PwD4Ctfk9o
\nHjWB7pQLUYpTZO9dm+4fpCMn9Okf43AE2yAOaAP94GdzdDJkxfciXKcsYr9Iluk
\nfaoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BUIGKMWXzuEd
\n3fy+1rCUwzOp9LSjtYf4ege
\n-----END PRIVATE KEY-----"
}
```

Example Response

- Example response 1

```
{
  "certificate": "-----BEGIN CERTIFICATE-----
\nMIIC4TCCAcmgAwIBAgICEREWdQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXID
\nb21wYW55IENBMB4XDTE4MDcwMjEzMDU0N1oXDTE4MTExNzEzMDU0N1owFDESMBAG
\nA1UEAwWJbG9jYWxob3N0MIIlBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAn0FQZgi3ucTX
+DNud1p/
b4XVM6l3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5\nu0U0NqPQZKUrZz3rQeLN9mYiUTJZPutYIFDDb
B8CtIgV+eyU9yYJslWx/
Bm5kWNPh9\n7B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lFCHkt/W7jaS
\nlAzlsD+QM6l7QjHwJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQyLYKy4zgnv1tn/K
\ny09cxLKAftgoZWQD2FAZJf9F7k1kYNwqITz3CPLZUUn7yw3nkOOTLMI28IEv0WY
\nYd7CMJQkS1NPJBKNOGfR/wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29t
\n\nhWQKuUvJhWwR/AAABMBMGGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCsGSIb3DQEBCwUA
\nA4IBAQA8IMQJxaTey7EjXtRSLVIEAMftAQPG6jijNQvIBQYUDauDT4W2XU25wAn
\n\njiOyQ83va672K1G9s8n6xlH+xwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDa
\n\nnezmcCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPRLYLzp1HMnl6hkjPk4PCZ
\n\nwKnha0dlScati9Cct3UzXSNJOSLalKdHErH08lqd+1BchScxChk0xNItn1HZZGml\n
+vbmunok3A2luc14rnsrckbGYqXGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZ\niYsGDVN
+9QBd0eYUHce+77s96i3\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+87kYwsMhRcgdcJ8KcnX1nf2Vl2ksXlTQ2o9BkpStnPntB4s32ZiJRMlk
+61iUUMNsHwk2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM
\nMD30gHh6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8lCq39buNplgDOWZEP5AqzXt
\n\nCOFYn6RTH5SRug4hKNN7sT1eYMsLHu7wtEBDKVgrLJOce/W2f8rLT1zEsoAW2Ch\n\nZAPYUBkl/
0XUWTRg3CohPPcl+UtlRSfvLDeeQ460swjbgwS/RbJh3slwLCRLU08k\nnEo04Z9H/
AgMBAAEcggEAEleaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/Hl
\n\nfvCARftGgMaYWPSPNCJRMXB7tPwpQu19esjz4Z/cR2Je4fTLPrffGUshFgZjv5OQB
\n\nZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr
\n\nnciu9YklNNEHu6uRJ5g/eGGX3KQynTvIhnOVGAJvjTXcoU6fm7gYdHAD6jk9l9m\n\nEGpfYI6AdHlwFZcT/
RNAXhP82lg2gUJSgAu66FFDjMwQXKbafKdP3zq4Up8a7Ale\n\nnkrquPtfV1vWklg
+bUFhgGaiAEYTpAUN9t2DVliijgQKBgQDnYMMsaF0r557CM1CT
\n\nXUqgCZo8MKeV2jf2drlxRRwRL33SksQbzAQ/qRLd7GP3sCGqvkvWY2FPdFYf8kx
\n\nGcCeZPcleZYQAM41pjtsaM8tVbLWVR8UtGBuQoPSPH7JNF3Tm/JH/fbwjpp7dt
\n\nJ7n8EzkRUNE6alMHOFeych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr
\n\nniWgTWHXPZuXQaYhpjXo6+IMI6DpExiDgBAkMzJGlvS7yQiYWU+wthAr9urbWYdGZ
\n\nIS6VjoTkF6r7VZoILXX0fbuXh6lm8K8lQRfBpJff56p9phMwaBpDNDrfpHB5utBU
\nxs40yldp6wKBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zf3bGSXU/jR4eB
\n\n1lVQhELGI9CbKSdzKM71GyElmix/T7FnSHIWLho1qVo6AQyduNWnAQD15pr8KAd
\n\nXGXAZZ1FQcb3KYa+2fflERmazdOTWjYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak\n\n/735uP20KKqhNehZpC2dJei7OilgRhCS/dKASUXHSW4fptBnUxACYocdDxtY4Vha\n\nfl7FPMdvGl8ioYbvlHFh+X0Xs9r1S8yeWnHoXMB6eXWmYKMrAoveLa+2cFm1Agf
\n\n7nLhA4R4lqm9lpV6SKegDUK4fxp9pPyodZPqBLLAoGBAJkD4wHW54PwD4Ctfk9o
\nHjWB7pQLUYpTZO9dm+4fpCMn9Okf43AE2yAOaAP94GdzdDJkxfciXKcsYr9Iluk
\nfaoXgjKR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BUIGKMWXzuEd
\n3fy+1rCUwzOp9LSjtYf4ege
\n-----END PRIVATE KEY-----"
}
```

```
\njHjWB7pQlUYpTZO9dm+4fpCMn9Okf43AE2yAOaAP94GdzdDJkxfciXKcsYr9Iluk
\nfaoXgjkR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BUIGKMWXzuEd\n3fy
+1rCUwzOp9LSjtYf4ege\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	Mandator y	Type	Description
project_id	Yes	Strin g	Specifies the project ID.
certificate_id	Yes	Strin g	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	Mandator y	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	Mandator y	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	Mandator y	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	Mandator y	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	Mandator y	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	Mandator y	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 unum 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"
}
```

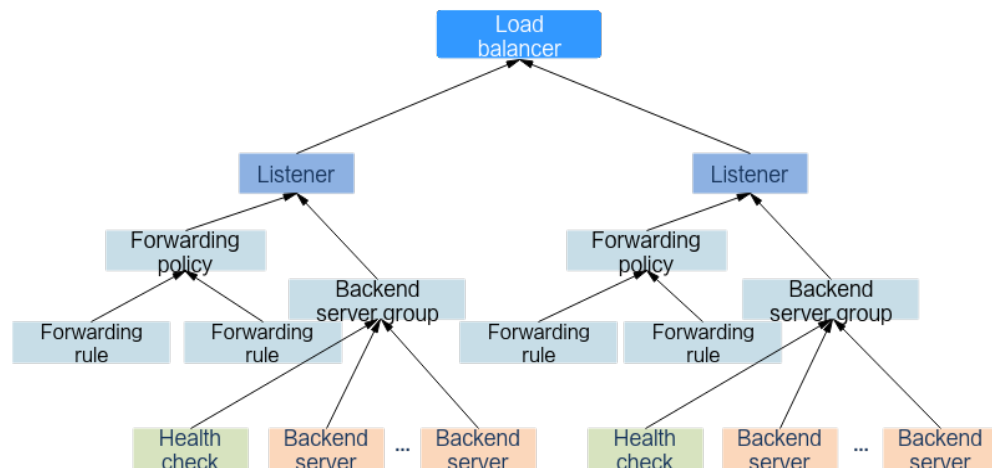
- If the request is abnormal, locate the fault by referring to [Error Codes](#).

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

Permi ssion	API	Action	IAM Project	Enterprise Project
Creat es a load balan cer	POST /v2/ {project_id}/elb/ loadbalancers	elb:loadbalanc ers:create	√	√
Queri es a load balan cer	GET /v2/ {project_id}/elb/ loadbalancers/ {loadbalancer_id}	elb:loadbalanc ers:get	√	√
Queri es the status tree of a load balan cer	GET /v2/ {project_id}/elb/ loadbalancers/ {loadbalancer_id}/ statuses	elb:loadbalanc ers: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	√	√

Permissi on	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

Permis sion	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
Create a forwarding rule	POST /v2/{project_id}/elb/l7policies/{l7policy_id}/rules	elb:l7rules:create	√	√
Query a forwarding rule	GET /v2/{project_id}/elb/l7policies/{l7policy_id}/rules/{l7rule_id}	elb:l7rules:get	√	√
Query forwarding rules	GET /v2/{project_id}/elb/l7policies/{l7policy_id}/rules	elb:l7rules:list	√	√
Update a forwarding rule	PUT /v2/{project_id}/elb/l7policies/{l7policy_id}/rules/{l7rule_id}	elb:l7rules:put	√	√
Delete 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	√	√
Query 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

Permi ssion	API	Action	IAM Project	Enterprise Project
Queri es defaul t resour ce quota s	GET /v2/{project_id}/elb/ quotas/defaults	elb:quotas :list	√	x
Queri es curren t resour ce quota s	GET /v2/{project_id}/elb/ quotas	elb:quotas :list	√	x

9.2.11 Tag

Permissio n	API	Action	IAM Project	Enterprise Project
Queries all tags of a load balancer.	GET /v2.0/{project_id}/ loadbalancers/ {loadbalancer_id}/tags	elb:loadbal ancerTags:g et	√	x
Adds or deletes load balancer tags in batches.	POST /v2.0/{project_id}/ loadbalancers/ {loadbalancer_id}/tags/ action	elb:loadbal ancerTags:c reate	√	x
Queries tags of all load balancers in a specific project.	GET /v2.0/{project_id}/ loadbalancers/tags	elb:loadbal ancerTags:g et	√	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

Permi ssion	API	Action	IAM Project	Enterprise Project
Creat es a load balan cer	POST /v3/ {project_id}/elb/ loadbalancers	elb:loadbalanc ers:create	√	√
Queri es a load balan cer	GET /v3/ {project_id}/elb/ loadbalancers/ {loadbalancer_id}	elb:loadbalanc ers:get	√	√
Queri es the status tree of a load balan cer	GET /v3/ {project_id}/elb/ loadbalancers/ {loadbalancer_id}/ statuses	elb:loadbalanc ers:get	√	√
Queri es load balan cers	GET /v3/ {project_id}/elb/ loadbalancers	elb:loadbalanc ers:list	√	√
Updat es a load balan cer	PUT /v3/ {project_id}/elb/ loadbalancers/ {loadbalancer_id}	elb:loadbalanc ers: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
Delete an IP address group	DELETE /v3/{project_id}/elb/ipgroups/{ipgroup_id}	elb:ipgroups:delete	√	√
Update IP addresses in an IP address group	PUT /v3/{project_id}/elb/ipgroups/{ipgroup_id}/iplist/create-or-update	elb:ipgroups:put	√	√
Delete 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
Create a certificate	POST /v3/{project_id}/elb/certificates	elb:certificates:create	√	√
Query a certificate	GET /v3/{project_id}/elb/certificates/{certificate_id}	elb:certificates:get	√	√
Query certificates	GET /v3/{project_id}/elb/certificates	elb:certificates:list	√	√
Modify 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

Permi ssion	API	Action	IAM Project	Enterprise Project
Quer ies the API versio n	GET /versions	elb:quotas :list	√	x

9.3.13 Availability Zone

Permi ssion	API	Action	IAM Project	Enterprise Project
Quer ies AZs	GET /v3/{project_id}/elb/ availability-zones	elb:availa bility- zones:list	√	√

9.3.14 Load Balancer Flavor

Permi ssion	API	Action	IAM Project	Enterprise Project
Quer ies defaul t resour ce quota s	GET /v3/{project_id}/elb/ flavors	elb:flavors :list	√	x
Quer ies curren t resour ce quota s	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 <i>YYYY-MM-DDTHH:MM:SS</i> 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 <i>YYYY-MM-DDTHH:MM:SS</i> 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
<code>vip_subnet_id</code>	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.
<code>provider</code>	No	String	Specifies the provider of the load balancer. The value can only be vlb .
<code>vip_address</code>	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.
<code>admin_state_up</code>	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
<code>id</code>	String	Specifies the ID of the associated listener.

Table 10-14 pools parameter description

Parameter	Type	Description
<code>id</code>	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
<code>vip_address</code>	No	String	Specifies the private IP address of the load balancer. This IP address must be the one in the subnet specified by <code>vip_subnet_id</code>. If this parameter is not specified, an IP address is automatically assigned to the load balancer from the subnet specified by <code>vip_subnet_id</code>. The value contains a maximum of 64 characters.
<code>admin_state_up</code>	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
<code>id</code>	String	Specifies the ID of the associated listener.

Table 10-20 pools parameter description

Parameter	Type	Description
<code>id</code>	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": "xxxxxxxx"
      },
      "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	Mandato ry	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 <i>YYYY-MM-DDTHH:MM:SS</i> 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 <i>YYYY-MM-DDTHH:MM:SS</i> 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: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:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:AES128-SHA:AES256-SHA

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 <i>YYYY-MM-DDTHH:MM:SS</i> format.
updated_at	String	Specifies the time when the listener was updated. The UTC time is in <i>YYYY-MM-DDTHH:MM:SS</i> 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 <i>YYYY-MM-DDTHH:MM:SS</i> 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 <i>YYYY-MM-DDTHH:MM:SS</i> 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"
  },
  {
    "id": "e385-4e39-83de-4dde1f801ccb",
    "name": "lsnr_name_mod",
    "protocol_port": 8080,
    "protocol": "HTTP",
    "description": "Listener for the application",
    "default_tls_container_ref": null,
    "sni_container_refs": [],
    "connection_limit": -1,
    "protocol_port": 8080,
    "default_pool_id": null,
    "id": "e385-4e39-83de-4dde1f801ccb",
    "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 <i>YYYY-MM-DDTHH:MM:SS</i> format.
updated_at	String	Specifies the time when the listener was updated. The UTC time is in <i>YYYY-MM-DDTHH:MM:SS</i> 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:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:AES128-SHA:AES256-SHA

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 <i>YYYY-MM-DDTHH:MM:SS</i> format.
updated_at	String	Specifies the time when the listener was updated. The UTC time is in <i>YYYY-MM-DDTHH:MM:SS</i> 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": null,  
    "healthmonitor_id": null,  
    "listeners": [],  
    "members": [],  
    "id": "4e496951-befb-47bf-9573-c1cd11825c07",  
    "name": ""  
  }  
}
```

```
{
  "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	Mandator y	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 <code>/</code>, and the value must start with a slash (<code>/</code>). This parameter is valid only when the value of type is set to HTTP. An example value is <code>/test</code>. 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	Mandator y	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	Mandator y	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 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.

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 <code>_~';@^-%#&\$.*+? ,=!: \\V()[]{}</code>

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 <code>_~';@^-%#&\$. *+?,=!: \() [] {}</code>

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 <code>_~';@^-%#&\$. *+?,=!: \()[]{}</code>
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 <code>_~!;@^-%#&\$.*+?,= : \()[]{}</code>

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 <code>_~';@^-%#&\$. *+? ,=!: \() [] {}</code>

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 <code>_~';@^-%#&\$.*+?,=!: \()[]{}</code>
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 <code>_~';@^-%#&\$.*+?,:! \(){}{}{ }</code>.

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 <code>_~';@^-%#&\$.*+?,=!: \()[]{}</code>
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 <i>YYYY-MM-DDTHH:MM:SS</i> format.
create_time	String	Specifies the time when the certificate was created. The UTC time is in <i>YYYY-MM-DDTHH:MM:SS</i> format.
update_time	String	Specifies the time when the certificate was updated. The UTC time is in <i>YYYY-MM-DDTHH:MM:SS</i> 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-----
    \nMIIEvglBADANBgkqhkiG9w0BAQEFAASCBAKgwggSkAgEAAoIBAQQDQVAbOLe5xNf4M
    \n253Wn9vhdUzojetjv4J+B7kYwsMhRcgdcJ8KCnX1nfzTvI2ksXITQ2o9BkpStnPe\ntB4s32ZiJRMlk
    +61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM
    \nMD30gLh6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8lcq39buNplgDOWzEP5AqzXt
    \nCOFYn6RTH5SRug4hKNN7sT1eYMsLHu7wtEBDKVgrLjOCe/W2f8rLT1zEsoAW2Ch\lnZAPYUBkl/
    0XuTWRg3CohPPcl+UtlRSfvLDeeQ460swjbgwS/RbJh3slwCRLU08k\neO04Z9H/
    AgMBAACGgEAEleaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/Hl
    \nfvCarftGgMaYWPSPNCJRMXB7tPwpQu19esjz4Z/cR2Je4fTLPrffGUshFgZjv5OQB
    \nZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr
    \nciu9YklnNEHu6uRJ5g/eGGX3KQynTvVIhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M\neGpfYI6AdHlwFZCT/
    RNAXhP82lg2gUJSgAu66FFdJmWQXKbafKdP3zq4Up8a7Ale\nkrguPtfV1vWklg
    +bUFhgGaiAEYTpAUN9t2DVIijgQKBgQDnYMMsaF0r557CM1CT
    \nXUqgCZo8MKeV2jf2drlxRRwRL33SksQbzAQ/qrLd7GP3sCGqvkvWY2FPdFyF8kx
    \nGcCeZPcleZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/fbwjP7dt
    \nJ7n8EzkRUNE6alMHOFEeych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr
    \niWgTWHXPZxUQaYhpjXo6+IMl6DpExiDgBAkMzJGlvS7yQiYWU+wthAr9urbWYdGZ
    \nIS6VjoTkF6r7VZolLX0fbuXh6lm8K8lQRfBpJff56p9phMwaBpDNDrfpHB5utBU
    \nxs40yldp6wKBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zJf3bGSXU/jR4eB
    \n1lVQhELG9CbKsdzKM71GyElmix/T7FnJSHIwlho1qVo6AQyduNWnAQD15pr8KAd
    \nXGAZZ1FQcb3KYa+2fflERmazedOTWjY0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak\n/
    735uP20KKqhNehZpC2dJei7OilgRhCS/dKASUXHSW4fptBnUxACYocdDxtY4Vha\nf1f7FPMdvGL8ioYbvlHFh
    +X0s9r1S8yeWnHoXMB6eXWmYKMrAoveLa+2cFm1Agf
    \n7nLhA4R4lqm9lpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAkJD4wHW54PwD4Ctfk9o
    \njHjWb7pQlUYpTZO9dm+4fPMn9Okf43AE2yAOaP94GdzdDJkxfciXKcsYr9lluk
    \nfaoXgjkR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BUIGKMWXzuEd\n3fy
    +1rCUwzOp9LSjtYf4ege\n-----END PRIVATE KEY-----",
  "certificate":
    "-----BEGIN CERTIFICATE-----
    \nMIICATCCAcmgAwIBAgIcERewDQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXID
    \nb21wYWV5IENBM4XDTE4MDcwMjEzMDU0N1oXDTQ1MTExNzEzMDU0N1owFDESMBAG
    \nA1UEAwJbG9jYWxob3N0MIIlBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAn0FQGi3ucTX
    +DNud1p/
    b4XVM6l3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5\nu0NqPQZKURzZ3rQeLN9mYiUTJZPutYlFDDb
    B8CtIgV+eyU9yYJslWx/
    Bm5kWNPh9\n7B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/W7jaS
    \nIaZlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylyKy4zgnv1tn/K
    \ny09cxLKAftgoZWQD2FAZJf9F7k1kYNwqlTz3CPILZUUn7ywnkOOTLMl28IEv0WY
    \nYd7CMJQkS1NPJBKNOGfR/wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29t
    \nhwQKuUvJhwr/AAABMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCsqGSIb3DQEBcWUA
    \nA4IBAQA8IMQJxaTey7EjXtRLSVIEAMftAQPG6ijNQuvIBQYUDauDT4W2XU25wAn
    \nIoyQ83va672K1G9s8n6xLH+xwwdSNnozaKzC87vwSeZKI0dl9I5I98TGKI6OoDa
    \nezmzCwQYtHBMVQ4c7ML8554Ft1mWst4dMAK2rzNyjvPRLYlp1Hmnl6hkjPk4PCZ
    \nnwKnha0dlScati9CCt3UzXSNJOSLalKdHErH08lqd+1BchScxChk0xNITn1HZZGml\n
    +vbmunok3A2lucl14rnsrbcGyqGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZ\niYsGDVN
    +9QBd0eYUHce+77s96i3l\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-----
  \nMIIEvglBADANBgkqhkiG9w0BAQEFAASCBAKgwggSkAgEAAoIBAQQDQVAbOLe5xNf4M
  \n253Wn9vhdUzojetjv4J+B7kYwsMhRcgdcJ8KCnX1nfzTvI2ksXITQ2o9BkpStnPe\ntB4s32ZiJRMlk
  +61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM
  \nMD30gLh6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8lcq39buNplgDOWzEP5AqzXt
```

```
\nCOFYn6RTH5SRug4hKNN7sT1eYMslHu7wtEBDKVgrLjOCe/W2f8rLT1zEsoAW2Chl\nZAPYUBkl/
0XuTWrg3CohPPcl+UtlRSfvLDeeQ460swjbgwS/RbJh3slwlCRLU08k\nEo04Z9H/
AgMBAAECggEAEleaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/Hl
\nfvCArftGgMaYWP5NCJRMXB7tPwpQu19esjz4Z/cR2Je4fTLPrffGUshFgZjv5OQB
\nZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr
\nnciu9YKlnNEHu6uRI5g/eGGX3KQynTvVlhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M\nnEGpfYI6AdHlwFZcT/
RNAXhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7Ale\nnkrgruPtFv1vWklg
+bUfhgGaiAEYTpAUN9t2DVIijgQKBgQDnYMMsaF0r557CM1CT
\nXUqgCZo8MKeV2jf2drlxRRwRL33SksQbzAQ/qRLd7GP3sCGqvkwWY2FPdFYf8kx
\nGcCeZPcleZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/fbwjpp7dt
\nJ7n8EzkRUNE6aIMHOFeeych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr
\nniWgTWHXPZxUQaYhpjXo6+IMl6DpExiDgBAkMzJGlvS7yQiyWU+wthAr9urbWYdGZ
\nlS6VjoTkF6r7VZolLXX0fbuXh6lm8K8lQRfBpjff56p9pMwaBpDNDrfpHB5utBU
\nxs4vYldp6wKBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zf3bGSXU/jR4eB
\nl1VQhELGI9CbKSdzKM71GyElmix/T7FnJSHIWIho1qVo6AQyduNWnAQD15pr8KAd
\nXGXAZZ1FQcb3KYa+2fflERmazdOTWjY0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak\n/
735uP20KKqhNehZpC2dJei7OilgRhCS/dKASUXHSW4fptBnUxACYocdDxtY4Vha\nnfl7FPMdvG8ioYbvlHFH
+X0Xs9r1S8yeWnHoXMB6eXWmYKMJrAoveLa+2cFm1Agf
\n7nLhA4R4lqm9lpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAjkD4wHW54PwD4Ctfk9o
\nhjHjWB7pQLUYpTZO9dm+4fpCMn9Okf43AE2yAOaAP94GdzDjKxfciXKcsYr9lluk
\nfaoXgjkR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BULGKMWXzuEd\nn3fy
+1rCUwzOp9LSjtYf4ege\n-----END PRIVATE KEY-----",
  "tenant_id": "930600df07ac4f66964004041bd3deaf",
  "type": "server",
  "certificate": "-----BEGIN CERTIFICATE-----
\nMIIC4TCCAcmgAwIBAgI CEREWdQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXID
\nnb21wYW55IENBMBA4XDTE4MDcwMjEzMDU0N1oXDTQ1MTExNzEzMDU0N1owFDESMBAG
\nA1UEAwWJbG9jYWxob3N0MIIlBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAn0FQGzi3ucTX
+DNud1p/
b4XVM6l3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5\nU0NqPQZKUrZz3rQeLN9mYiUTJZPutYlFDDb
B8CtIgV+eyU9yYJslWx/
Bm5kWNPh9\n7B9Y9pbbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/W7jaS
\nlAzlsxD+QM6L7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylyKy4zgnv1tn/K
\ny09cxLKAftgoZWQD2FAZJf9F7k1kYNwqlTz3CPILZUUn7yw3nkOOTLMI28IEv0WY
\nYd7CMJQkS1NPJBKNOGfR/wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29t
\nnhwQKuUvJhwR/AAABMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCsGSIb3DQEBCwUA
\nA4IBAQA8lMQxaTey7EjXtRLSVIEAMftAQPG6ijNQuvIBQYUDauDT4W2XUZ5wAn
\nnjiOyQ83va672K1G9s8n6xLH+xwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDa
\nnezmcwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPRLYLzp1HMn16hkjPk4PCZ
\nnwKnha0dlScati9CCt3UzXSNJOSLaKdHErH08lqd+1BchScxChk0xNiTn1HZZGml\n
+vbmunok3A2luc14rnsrckbGYqGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZ\nniysGDVN
+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 <i>YYYY-MM-DD HH:MM:SS</i> format.
update_time	No	String	Specifies the time when the certificate was updated. The UTC time is in <i>YYYY-MM-DD HH:MM:SS</i> 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 <i>YYYY-MM-DD HH:MM:SS</i> format.
create_time	String	Specifies the time when the certificate was created. The UTC time is in <i>YYYY-MM-DD HH:MM:SS</i> format.
update_time	String	Specifies the time when the certificate was updated. The UTC time is in <i>YYYY-MM-DD HH:MM:SS</i> 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-----
\nMIIC4TCCAcmgAwIBAgIcEREWdQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMTXID
\nb21wYW50IENBM4XDTE4MDcwMjEzMTExNzEzMTExNzEzMTExNzEzMTExNzEzMTEx
\nA1UEAwWJbG9jYWxob3N0MIIlBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
+DNud1p/
b4XVM6l3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5\nU0NqPQZKURzZ3rQeLN9mYiUTJZPutYlFDDb
B8CtIgv+eyU9yYJslWx/
Bm5kWNPh9\n7B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/W7jaS
\nlA1zlsxD+QM6l7QjhwJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylyKy4zgnv1tn/K
\ny09cxLKAftgoZWQD2FAZJf9F7k1kYNwqlTz3CPILZUUn7yw3nkOOTLMl28IEv0WY
\nYd7CMJQkS1NPJBKNOGfR/wIDAQABozowODAhBgNVHREEGjAYggpkb21hW4uY29t
\nnhwQKuUvJhwr/AAABMBMGA1UdJQMMMAoGCCsGAQUFBwMBMA0GCsqGSIb3DQEBcWUA
\nA4lBAQA8lMQJxaTey7EjXtRLSVIEAMftAQPG6ijNQuvIBQYUDauDT4W2XU5wAn
\nnjiOyQ83va672K1G9s8n6xlH+xwwdSNnozaKzC87vwSeZKI0dl9I5I98TGKI6OoDa
\nnezmcwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPRLYLp1HMnl6hkpK4PCZ
\nnwKnha0dlScati9CCt3UzXSNJOSLalKdHErH08lqd+1BchScxChk0xNITn1HZZGml\n
+vbmunok3A2lucl14nsrcbkGYqXGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZ\niYsGDVN
+9QBd0eYUHce+77s96i3l\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-----
\nMIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKggggSkAgEAAoIBAQDQVAbOLe5xNf4M
\n253Wn9vhdUzojetjv4J+B7kYwsMhRcgdcJ8KcN1nfzTvl2ksXlTQ2o9BkpStnPntB4s32ZiJRMlk
+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM
\nMD30gH6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8lcq39buNplgDOWzEP5AqzXt
\nnCOFYn6RTH5SRug4hKNN7sT1eYMsLHu7wtEBDKVgrLJOce/W2f8rLT1zEs0AW2Chl\nnZAPYUBkl/
0XuTWRg3CohPPcl+UtlRSfVLDeeQ460swjbgwS/RbJh3slwLCRLU08k\nnEo04Z9H/
AgMBAAECCgEAEleaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/HL
\nnfvcArftGgMaYWPNSNCJRMXB7tPwpQu19esjz4Z/cR2Je4fTLPrffGUshFgZjv5OQB
\nnZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr
\nnciu9YklnNEHu6uRJ5g/eGGX3KQynTvVlhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M\nnEGpfYI6AdHlwFZcT/
RNAxhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7Ale\nnkrquPtfV1vWklg
+bUfhgGaiAEYTpAUN9t2DVIiijgQKBgQDnYMMsaF0r557CM1CT
\nXUqgCZo8MKeV2jf2drlxRRwRL33SksQbzAQ/qrLd7GP3sCGqvkvxWY2FPdFYf8kx
\nGcCeZPcleZYQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/fbwjppJ7dt
\nnJ7n8EzkRUNE6alMHOFEeych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr
\nniWgTWHXPZxUQaYhpjXo6+IMI6DpExiDgBAkMzJGlvS7yQiYWU+wthAr9urbWYdGZ
\nnLS6VjoTkF6r7VZoLXX0fbuXh6lm8K8lQRfBpJff56p9phMwaBpDNDrfpHB5utBU
\nnxs40yldp6wKBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zJf3bGSXU/jR4eB
\nn1lVQhELGI9CbKsDzKM71GyElmix/T7FnJSHIWLho1qVo6AQyduNWnAQD15pr8KAd
\nnXGAZZ1FQcb3KYa+2fflERmazdOTWjYz0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak\nn/
735uP20KKqhNehZpC2dJei7OilgRhCS/dKASUXHSW4fptBnUxACYocdDxtY4Vha\nnfl7FPMdvGL8ioYbvlHFH
+X0Xs9r1S8yeWnHoXMB6eXWmYKMMjrAoveLa+2cFm1Agf
\n7nLhA4R4lqm9lpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAJkD4wHW54PwD4Ctfk9o
\nnjHjWB7pQlUYpTZO9dm+4fpCMn9Okf43AE2yAOaAP94GdzdDJkxfciXKcsYr9Iluk
\nnfaoXgJkR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BUlGKMWXzuEd\nn3fy
+1rCUwzOp9LSjtYf4ege\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-----  
MIIFizCCBHOGAwIBAgIQBlQycV3bWsVsCttw5rgRjANBgkqhkiG9w0BAQsFADBu  
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3  
d3cuZGlnaWNlcnQuY29tMS0wKwYDVQQDEyRfBmNyeXB0aW9uIEV2ZXJ5d2hlcuUg  
RFYgVExTIENBIC0gRzEwHhcNMTgwNzEwMDAwMDAwWHcNMTkwNzEwMTIwMDAwWjAUMRlwEAYDVQQDEwlpY2UxMjMudGswggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK  
AoIBAQCTdIQMoAvylnR6X1dihhNwbdGesbMW6NZX7ffpj9XrB3KCqqlxz14VmH9  
PntvrPLJNeolgLqDZZc4zKbUkmqxY1dvGds41coKzdtc9lg23GVK48wfesnk5r50  
afyU52R1JISHDOhiDhHOSyhrOzc2GreLrByWKFUaAue6rTnyMbZQaSPtrTAqsURZ  
wcmJ6R3A6JwokOgxXBSu41ufPQIFkMgxygKxEBLzJlJlRqCXQHXYoxbsTyolb6jwp  
w4H6vcRIEcFags98ApWRoEKjy7eOP3UUm05F+OkOvXhrLxEqIPm/rlwE0PmVlmm9  
DgBaFyb3xT/MtT2VRSfCJQHglcsdAgMBAAGgggJ9MIICeTafBgNVHSMEGDAWgBRV  
dE+yck/1YLpQ0dfmUVyaAYca1zAdBgNVHQ4EFgQUEFavzYXBNbIHbchbaKcUKad+  
qCEwIwYDVR0RBwwGolJaWNlMTIzLnRrgg13d3cuaWNlMTIzLnRrMA4GA1UdDwEB  
/wQEAWIfoDAdBgNVHSUEFjAUBgggBgEFBQcDAQYIKwYBBQUHAWIwTAYDVRO0BEUw  
QzA3BgIghkgBhv1sAQIwKjAoBggrBgEFBQcCARYcaHR0cHM6Ly93d3cuZGlnaWNl  
cnQuY29tL0NQZuZAIgZngQwBAgEwgYEGCCsGAQUFBwEBBHUwczAlBggrBgEFBQcw  
AYYZaHR0cDovL29jc3AyLmRpZ2ljZXJ0LmNvbTBKbGgrBgEFBQcwAoY+aHR0cDov  
L2NhY2VydHMuZGlnaWNlcnQuY29tL0Vud3J5c3Rpb25fZmVyeXdoZXJIRFZUTFND  
Q51HMS5jcnQwCQYDVROTBAlwADCCAQQGCisGAQQB1nkCBAIEgfUEgfIA8AB2AKS5  
CZC0GFgUUh7sTosxncAo8NZgE+RvfuON3zQ7IDdwQAAABZIOncLCAAAQDAEcwRQIh  
AJX6gCXNggPdfoFdtZpZlYr64TTrR/+b9QKKhyJ2EjBAiAWgu3BG2QK9tWQXPUN  
IfadC0nvqmDovabg5nmRMan2mQB2Ald1v+dZfPiMQ5lfvNu/1aNR1Y2/0q1YMG0  
6v9eolMPAAABZIOncLQEAQAQDAEcwRQIhAJVRe/7n88dD6KdhNrd4LdFjGARQNmta  
Y/K2dFDQXPSfAiBOLrWW8unHOL25RWHJU7Ost3XkNhQYtrLDJrnzo/9kZzANBgkq  
hkiG9w0BAQsFAAOCAQEAEqT9XcHmj4OnNAk0IGmF3nKS/u/UgGsY4EJfXwQY2bTZ  
PCkqxQOA6HEX59vJ+UilTojrNDi0WskRm/8SKBhtMwzWzX3ile8KiR6ffFqHPUTV  
XHZctfAFo47c7axqon8vumMLEv1PxVlmivQ446K7z3kGm34dhMYxS4Gz2gTl8IKt  
90OegejuhbAs5Wlvp1BK8HLYIb5+mw+cgkUC9KtALs5qVbWzogs0bS20KaYarGcu  
otcZAOMeJdBFWnpzhr1fxmjaNY4u4hrqPZSTU/iBjdHapoza3zAffxysmGYqs9dR  
jFyxZeR4scz8GqSTFviNdH9jvtDJkdAC5hfMaB811Q==  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
MIIEqjCCA5KgAwIBAgIQAnmsRYvBskWr+YBTzSybsTANBgkqhkiG9w0BAQsFADBh  
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3  
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDEXdEaWdpQ2VydCBHbG9iYWwUgU9vdCBD  
QTAEFw0xNzExMjcxMjQ2MTBaFw0yNzExMjcxMjQ2MTBaMG4xCzAJBgNVBAYTAiVT  
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j  
b20xLTArBgNVBAMTJEVud3J5c3Rpb24gRXZlcnlnaG9wYyZSBEViBUTFMgQ0EgLSBH  
MTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALPeP6wkb41dyQh6mKc  
oHqt3jRlxW5MDvf9QyIOR7VfFwK656es0UFilb74N9pRntzF1UgYzDGu3ppZVMdo  
lbxhm6dWS9OK/LfehKNT0OYI9aqk6F+U7cA6jxSC+iDBPXwdF4rs3KRyp3aQn6pj  
pp1yr7IB6Y4zv72Ee/PLZ/6rK6InC6WpK0nPV0YR7n9iDuPe1E4lxUMBH/T33+3h  
yuH3dvfgiWUOUkjdpMbyxX+XNle5uEliYBsi4lvbcTch8ruifCii5mDXkZrnMT8n  
wfYCV6v6kDdXkbgGRLKsR4pucbJtbKqlKUGxuZl2t7pfewKRc5nWecvDBZF3+1M  
pA8CAwEAAaOCAU8wggFLMB0GA1UdDgQWBBrVdE+yck/1YLpQ0dfmUVyaAYca1zAf  
BgNVHSMEGDAWgBQD3IA1VtFMu2bwo+lbG8OXsj3RVTAOBgNVHQ8BAf8EBAMCAYYw  
HQYDVROlBBYwFAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBHMCMBlGA1UdEwEB/wQIMAYBAf8C  
AQAwNAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBzABhhodHRwOi8vb2Nzc5kaWdp  
Y2VydC5jb20wYyZSBEViBUTFMgQ0EgLSBHMTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALPeP6wkb41dyQh6mKc  
oHqt3jRlxW5MDvf9QyIOR7VfFwK656es0UFilb74N9pRntzF1UgYzDGu3ppZVMdo  
lbxhm6dWS9OK/LfehKNT0OYI9aqk6F+U7cA6jxSC+iDBPXwdF4rs3KRyp3aQn6pj  
pp1yr7IB6Y4zv72Ee/PLZ/6rK6InC6WpK0nPV0YR7n9iDuPe1E4lxUMBH/T33+3h  
yuH3dvfgiWUOUkjdpMbyxX+XNle5uEliYBsi4lvbcTch8ruifCii5mDXkZrnMT8n  
wfYCV6v6kDdXkbgGRLKsR4pucbJtbKqlKUGxuZl2t7pfewKRc5nWecvDBZF3+1M  
pA8CAwEAAaOCAU8wggFLMB0GA1UdDgQWBBrVdE+yck/1YLpQ0dfmUVyaAYca1zAf  
BgNVHSMEGDAWgBQD3IA1VtFMu2bwo+lbG8OXsj3RVTAOBgNVHQ8BAf8EBAMCAYYw  
HQYDVROlBBYwFAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBHMCMBlGA1UdEwEB/wQIMAYBAf8C  
AQAwNAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBzABhhodHRwOi8vb2Nzc5kaWdp  
Y2VydC5jb20wYyZSBEViBUTFMgQ0EgLSBHMTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALPeP6wkb41dyQh6mKc  
oHqt3jRlxW5MDvf9QyIOR7VfFwK656es0UFilb74N9pRntzF1UgYzDGu3ppZVMdo  
lbxhm6dWS9OK/LfehKNT0OYI9aqk6F+U7cA6jxSC+iDBPXwdF4rs3KRyp3aQn6pj  
pp1yr7IB6Y4zv72Ee/PLZ/6rK6InC6WpK0nPV0YR7n9iDuPe1E4lxUMBH/T33+3h  
yuH3dvfgiWUOUkjdpMbyxX+XNle5uEliYBsi4lvbcTch8ruifCii5mDXkZrnMT8n  
wfYCV6v6kDdXkbgGRLKsR4pucbJtbKqlKUGxuZl2t7pfewKRc5nWecvDBZF3+1M  
pA8CAwEAAaOCAU8wggFLMB0GA1UdDgQWBBrVdE+yck/1YLpQ0dfmUVyaAYca1zAf  
BgNVHSMEGDAWgBQD3IA1VtFMu2bwo+lbG8OXsj3RVTAOBgNVHQ8BAf8EBAMCAYYw  
HQYDVROlBBYwFAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBHMCMBlGA1UdEwEB/wQIMAYBAf8C  
AQAwNAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBzABhhodHRwOi8vb2Nzc5kaWdp  
Y2VydC5jb20wYyZSBEViBUTFMgQ0EgLSBHMTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALPeP6wkb41dyQh6mKc  
oHqt3jRlxW5MDvf9QyIOR7VfFwK656es0UFilb74N9pRntzF1UgYzDGu3ppZVMdo  
lbxhm6dWS9OK/LfehKNT0OYI9aqk6F+U7cA6jxSC+iDBPXwdF4rs3KRyp3aQn6pj  
pp1yr7IB6Y4zv72Ee/PLZ/6rK6InC6WpK0nPV0YR7n9iDuPe1E4lxUMBH/T33+3h  
yuH3dvfgiWUOUkjdpMbyxX+XNle5uEliYBsi4lvbcTch8ruifCii5mDXkZrnMT8n  
wfYCV6v6kDdXkbgGRLKsR4pucbJtbKqlKUGxuZl2t7pfewKRc5nWecvDBZF3+1M  
pA8CAwEAAaOCAU8wggFLMB0GA1UdDgQWBBrVdE+yck/1YLpQ0dfmUVyaAYca1zAf  
BgNVHSMEGDAWgBQD3IA1VtFMu2bwo+lbG8OXsj3RVTAOBgNVHQ8BAf8EBAMCAYYw  
HQYDVROlBBYwFAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBHMCMBlGA1UdEwEB/wQIMAYBAf8C  
AQAwNAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBzABhhodHRwOi8vb2Nzc5kaWdp  
Y2VydC5jb20wYyZSBEViBUTFMgQ0EgLSBHMTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALPeP6wkb41dyQh6mKc  
oHqt3jRlxW5MDvf9QyIOR7VfFwK656es0UFilb74N9pRntzF1UgYzDGu3ppZVMdo  
lbxhm6dWS9OK/LfehKNT0OYI9aqk6F+U7cA6jxSC+iDBPXwdF4rs3KRyp3aQn6pj  
pp1yr7IB6Y4zv72Ee/PLZ/6rK6InC6WpK0nPV0YR7n9iDuPe1E4lxUMBH/T33+3h  
yuH3dvfgiWUOUkjdpMbyxX+XNle5uEliYBsi4lvbcTch8ruifCii5mDXkZrnMT8n  
wfYCV6v6kDdXkbgGRLKsR4pucbJtbKqlKUGxuZl2t7pfewKRc5nWecvDBZF3+1M  
pA8CAwEAAaOCAU8wggFLMB0GA1UdDgQWBBrVdE+yck/1YLpQ0dfmUVyaAYca1zAf  
BgNVHSMEGDAWgBQD3IA1VtFMu2bwo+lbG8OXsj3RVTAOBgNVHQ8BAf8EBAMCAYYw  
HQYDVROlBBYwFAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBHMCMBlGA1UdEwEB/wQIMAYBAf8C  
AQAwNAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBzABhhodHRwOi8vb2Nzc5kaWdp  
Y2VydC5jb20wYyZSBEViBUTFMgQ0EgLSBHMTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALPeP6wkb41dyQh6mKc  
oHqt3jRlxW5MDvf9QyIOR7VfFwK656es0UFilb74N9pRntzF1UgYzDGu3ppZVMdo  
lbxhm6dWS9OK/LfehKNT0OYI9aqk6F+U7cA6jxSC+iDBPXwdF4rs3KRyp3aQn6pj  
pp1yr7IB6Y4zv72Ee/PLZ/6rK6InC6WpK0nPV0YR7n9iDuPe1E4lxUMBH/T33+3h  
yuH3dvfgiWUOUkjdpMbyxX+XNle5uEliYBsi4lvbcTch8ruifCii5mDXkZrnMT8n  
wfYCV6v6kDdXkbgGRLKsR4pucbJtbKqlKUGxuZl2t7pfewKRc5nWecvDBZF3+1M  
pA8CAwEAAaOCAU8wggFLMB0GA1UdDgQWBBrVdE+yck/1YLpQ0dfmUVyaAYca1zAf  
BgNVHSMEGDAWgBQD3IA1VtFMu2bwo+lbG8OXsj3RVTAOBgNVHQ8BAf8EBAMCAYYw  
HQYDVROlBBYwFAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBHMCMBlGA1UdEwEB/wQIMAYBAf8C  
AQAwNAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBzABhhodHRwOi8vb2Nzc5kaWdp  
Y2VydC5jb20wYyZSBEViBUTFMgQ0EgLSBHMTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALPeP6wkb41dyQh6mKc  
oHqt3jRlxW5MDvf9QyIOR7VfFwK656es0UFilb74N9pRntzF1UgYzDGu3ppZVMdo  
lbxhm6dWS9OK/LfehKNT0OYI9aqk6F+U7cA6jxSC+iDBPXwdF4rs3KRyp3aQn6pj  
pp1yr7IB6Y4zv72Ee/PLZ/6rK6InC6WpK0nPV0YR7n9iDuPe1E4lxUMBH/T33+3h  
yuH3dvfgiWUOUkjdpMbyxX+XNle5uEliYBsi4lvbcTch8ruifCii5mDXkZrnMT8n  
wfYCV6v6kDdXkbgGRLKsR4pucbJtbKqlKUGxuZl2t7pfewKRc5nWecvDBZF3+1M  
pA8CAwEAAaOCAU8wggFLMB0GA1UdDgQWBBrVdE+yck/1YLpQ0dfmUVyaAYca1zAf  
BgNVHSMEGDAWgBQD3IA1VtFMu2bwo+lbG8OXsj3RVTAOBgNVHQ8BAf8EBAMCAYYw  
HQYDVROlBBYwFAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBHMCMBlGA1UdEwEB/wQIMAYBAf8C  
AQAwNAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBzABhhodHRwOi8vb2Nzc5kaWdp  
Y2VydC5jb20wYyZSBEViBUTFMgQ0EgLSBHMTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALPeP6wkb41dyQh6mKc  
oHqt3jRlxW5MDvf9QyIOR7VfFwK656es0UFilb74N9pRntzF1UgYzDGu3ppZVMdo  
lbxhm6dWS9OK/LfehKNT0OYI9aqk6F+U7cA6jxSC+iDBPXwdF4rs3KRyp3aQn6pj  
pp1yr7IB6Y4zv72Ee/PLZ/6rK6InC6WpK0nPV0YR7n9iDuPe1E4lxUMBH/T33+3h  
yuH3dvfgiWUOUkjdpMbyxX+XNle5uEliYBsi4lvbcTch8ruifCii5mDXkZrnMT8n  
wfYCV6v6kDdXkbgGRLKsR4pucbJtbKqlKUGxuZl2t7pfewKRc5nWecvDBZF3+1M  
pA8CAwEAAaOCAU8wggFLMB0GA1UdDgQWBBrVdE+yck/1YLpQ0dfmUVyaAYca1zAf  
BgNVHSMEGDAWgBQD3IA1VtFMu2bwo+lbG8OXsj3RVTAOBgNVHQ8BAf8EBAMCAYYw  
HQYDVROlBBYwFAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBHMCMBlGA1UdEwEB/wQIMAYBAf8C  
AQAwNAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBzABhhodHRwOi8vb2Nzc5kaWdp  
Y2VydC5jb20wYyZSBEViBUTFMgQ0EgLSBHMTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALPeP6wkb41dyQh6mKc  
oHqt3jRlxW5MDvf9QyIOR7VfFwK656es0UFilb74N9pRntzF1UgYzDGu3ppZVMdo  
lbxhm6dWS9OK/LfehKNT0OYI9aqk6F+U7cA6jxSC+iDBPXwdF4rs3KRyp3aQn6pj  
pp1yr7IB6Y4zv72Ee/PLZ/6rK6InC6WpK0nPV0YR7n9iDuPe1E4lxUMBH/T33+3h  
yuH3dvfgiWUOUkjdpMbyxX+XNle5uEliYBsi4lvbcTch8ruifCii5mDXkZrnMT8n  
wfYCV6v6kDdXkbgGRLKsR4pucbJtbKqlKUGxuZl2t7pfewKRc5nWecvDBZF3+1M  
pA8CAwEAAaOCAU8wggFLMB0GA1UdDgQWBBrVdE+yck/1YLpQ0dfmUVyaAYca1zAf  
BgNVHSMEGDAWgBQD3IA1VtFMu2bwo+lbG8OXsj3RVTAOBgNVHQ8BAf8EBAMCAYYw  
HQYDVROlBBYwFAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBHMCMBlGA1UdEwEB/wQIMAYBAf8C  
AQAwNAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBzABhhodHRwOi8vb2Nzc5kaWdp  
Y2VydC5jb20wYyZSBEViBUTFMgQ0EgLSBHMTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALPeP6wkb41dyQh6mKc  
oHqt3jRlxW5MDvf9QyIOR7VfFwK656es0UFilb74N9pRntzF1UgYzDGu3ppZVMdo  
lbxhm6dWS9OK/LfehKNT0OYI9aqk6F+U7cA6jxSC+iDBPXwdF4rs3KRyp3aQn6pj  
pp1yr7IB6Y4zv72Ee/PLZ/6rK6InC6WpK0nPV0YR7n9iDuPe1E4lxUMBH/T33+3h  
yuH3dvfgiWUOUkjdpMbyxX+XNle5uEliYBsi4lvbcTch8ruifCii5mDXkZrnMT8n  
wfYCV6v6kDdXkbgGRLKsR4pucbJtbKqlKUGxuZl2t7pfewKRc5nWecvDBZF3+1M  
pA8CAwEAAaOCAU8wggFLMB0GA1UdDgQWBBrVdE+yck/1YLpQ0dfmUVyaAYca1zAf  
BgNVHSMEGDAWgBQD3IA1VtFMu2bwo+lbG8OXsj3RVTAOBgNVHQ8BAf8EBAMCAYYw  
HQYDVROlBBYwFAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBHMCMBlGA1UdEwEB/wQIMAYBAf8C  
AQAwNAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBzABhhodHRwOi8vb2Nzc5kaWdp  
Y2VydC5jb20wYyZSBEViBUTFMgQ0EgLSBHMTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALPeP6wkb41dyQh6mKc  
oHqt3jRlxW5MDvf9QyIOR7VfFwK656es0UFilb74N9pRntzF1UgYzDGu3ppZVMdo  
lbxhm6dWS9OK/LfehKNT0OYI9aqk6F+U7cA6jxSC+iDBPXwdF4rs3KRyp3aQn6pj  
pp1yr7IB6Y4zv72Ee/PLZ/6rK6InC6WpK0nPV0YR7n9iDuPe1E4lxUMBH/T33+3h  
yuH3dvfgiWUOUkjdpMbyxX+XNle5uEliYBsi4lvbcTch8ruifCii5mDXkZrnMT8n  
wfYCV6v6kDdXkbgGRLKsR4pucbJtbKqlKUGxuZl2t7pfewKRc5nWecvDBZF3+1M  
pA8CAwEAAaOCAU8wggFLMB0GA1UdDgQWBBrVdE+yck/1YLpQ0dfmUVyaAYca1zAf  
BgNVHSMEGDAWgBQD3IA1VtFMu2bwo+lbG8OXsj3RVTAOBgNVHQ8BAf8EBAMCAYYw  
HQYDVROlBBYwFAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBHMCMBlGA1UdEwEB/wQIMAYBAf8C  
AQAwNAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBzABhhodHRwOi8vb2Nzc5kaWdp  
Y2VydC5jb20wYyZSBEViBUTFMgQ0EgLSBHMTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALPeP6wkb41dyQh6mKc  
oHqt3jRlxW5MDvf9QyIOR7VfFwK656es0UFilb74N9pRntzF1UgYzDGu3ppZVMdo  
lbxhm6dWS9OK/LfehKNT0OYI9aqk6F+U7cA6jxSC+iDBPXwdF4rs3KRyp3aQn6pj  
pp1yr7IB6Y4zv72Ee/PLZ/6rK6InC6WpK0nPV0YR7n9iDuPe1E4lxUMBH/T33+3h  
yuH3dvfgiWUOUkjdpMbyxX+XNle5uEliYBsi4lvbcTch8ruifCii5mDXkZrnMT8n  
wfYCV6v6kDdXkbgGRLKsR4pucbJtbKqlKUGxuZl2t7pfewKRc5nWecvDBZF3+1M  
pA8CAwEAAaOCAU8wggFLMB0GA1UdDgQWBBrVdE+yck/1YLpQ0dfmUVyaAYca1zAf  
BgNVHSMEGDAWgBQD3IA1VtFMu2bwo+lbG8OXsj3RVTAOBgNVHQ8BAf8EBAMCAYYw  
HQYDVROlBBYwFAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBHMCMBlGA1UdEwEB/wQIMAYBAf8C  
AQAwNAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBzABhhodHRwOi8vb2Nzc5kaWdp  
Y2VydC5jb20wYyZSBEViBUTFMgQ0EgLSBHMTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALPeP6wkb41dyQh6mKc  
oHqt3jRlxW5MDvf9QyIOR7VfFwK656es0UFilb74N9pRntzF1UgYzDGu3ppZVMdo  
lbxhm6dWS9OK/LfehKNT0OYI9aqk6F+U7cA6jxSC+iDBPXwdF4rs3KRyp3aQn6pj  
pp1yr7IB6Y4zv72Ee/PLZ/6rK6InC6WpK0nPV0YR7n9iDuPe1E4lxUMBH/T33+3h  
yuH3dvfgiWUOUkjdpMbyxX+XNle5uEliYBsi4lvbcTch8ruifCii5mDXkZrnMT8n  
wfYCV6v6kDdXkbgGRLKsR4pucbJtbKqlKUGxuZl2t7pfewKRc5nWecvDBZF3+1M  
pA8CAwEAAaOCAU8wggFLMB0GA1UdDgQWBBrVdE+yck/1YLpQ0dfmUVyaAYca1zAf  
BgNVHSMEGDAWgBQD3IA1VtFMu2bwo+lbG8OXsj3RVTAOBgNVHQ8BAf8EBAMCAYYw  
HQYDVROlBBYwFAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBHMCMBlGA1UdEwEB/wQIMAYBAf8C  
AQAwNAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBzABhhodHRwOi8vb2Nzc5kaWdp  
Y2VydC5jb20wYyZSBEViBUTFMgQ0EgLSBHMTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALPeP6wkb41dyQh6mKc  
oHqt3jRlxW5MDvf9QyIOR7VfFwK656es0UFilb74N9pRntzF1UgYzDGu3ppZVMdo  
lbxhm6dWS9OK/LfehKNT0OYI9aqk6F+U7cA6jxSC+iDBPXwdF4rs3KRyp3aQn6pj  
pp1yr7IB6Y4zv72Ee/PLZ/6rK6InC6WpK0nPV0YR7n9iDuPe1E4lxUMBH/T33+3h  
yuH3dvfgiWUOUkjdpMbyxX+XNle5uEliYBsi4lvbcTch8ruifCii5mDXkZrnMT8n  
wfYCV6v6kDdXkbgGRLKsR4pucbJtbKqlKUGxuZl2t7pfewKRc5nWecvDBZF3+1M  
pA8CAwEAAaOCAU8wggFLMB0GA1UdDgQWBBrVdE+yck/1YLpQ0dfmUVyaAYca1zAf  
BgNVHSMEGDAWgBQD3IA1VtFMu2bwo+lbG8OXsj3RVTAOBgNVHQ8BAf8EBAMCAYYw  
HQYDVROlBBYwFAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBHMCMBlGA1UdEwEB/wQIMAYBAf8C  
AQAwNAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBzABhhodHRwOi8vb2Nzc5kaWdp  
Y2VydC5jb20wYyZSBEViBUTFMgQ0EgLSBHMTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALPeP6wkb41dyQh6mKc  
oHqt3jRlxW5MDvf9QyIOR7VfFwK656es0UFilb74N9pRntzF1UgYzDGu3ppZVMdo  
lbxhm6dWS9OK/LfehKNT0OYI9aqk6F+U7cA6jxSC+iDBPXwdF4rs3KRyp3aQn6pj  
pp1yr7IB6Y4zv72Ee/PLZ/6rK6InC6WpK0nPV0YR7n9iDuPe1E4lxUMBH/T33+3h  
yuH3dvfgiWUOUkjdpMbyxX+XNle5uEliYBsi4lvbcTch8ruifCii5mDXkZrnMT8n  
wfYCV6v6kDdXkbgGRLKsR4pucbJtbKqlKUGxuZl2t7pfewKRc5nWecvDBZF3+1M  
pA8CAwEAAaOCAU8wggFLMB0GA1UdDgQWBBrVdE+yck/1YLpQ0dfmUVyaAYca1zAf  
BgNVHSMEGDAWgBQD3IA1VtFMu2bwo+lbG8OXsj3RVTAOBgNVHQ8BAf8EBAMCAYYw  
HQYDVROlBBYwFAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBHMCMBlGA1UdEwEB/wQIMAYBAf8C  
AQAwNAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBzABhhodHRwOi8vb2Nzc5kaWdp  
Y2VydC5jb20wYyZSBEViBUTFMgQ0EgLSBHMTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALPeP6wkb41dyQh6mKc  
oHqt3jRlxW5MDvf9QyIOR7VfFwK656es0UFilb74N9pRntzF1UgYzDGu3ppZVMdo  
lbxhm6dWS9OK/LfehKNT0OYI9aqk6F+U7cA6jxSC+iDBPXwdF4rs3KRyp3aQn6pj  
pp1yr7IB6Y4zv72Ee/PLZ/6rK6InC6WpK0nPV0YR7n9iDuPe1E4lxUMBH/T33+3h  
yuH3dvfgiWUOUkjdpMbyxX+XNle5uEliYBsi4lvbcTch8ruifCii5mDXkZrnMT8n  
wfYCV6v6kDdXkbgGRLKsR4pucbJtbKqlKUGxuZl2t7pfewKRc5nWecvDBZF3+1M  
pA8CAwEAAaOCAU8wggFLMB0GA1UdDgQWBBrVdE+yck/1YLpQ0dfmUVyaAYca1zAf  
BgNVHSMEGDAWgBQD3IA1VtFMu2bwo+lbG8OXsj3RVTAOBgNVHQ8BAf8EBAMCAYYw  
HQYDVROlBBYwFAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBHMCMBlGA1UdEwEB/wQIMAYBAf8C  
AQAwNAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBzABhhodHRwOi8vb2Nzc5kaWdp  
Y2VydC5jb20wYyZSBEViBUTFMgQ0EgLSBHMTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALPeP6wkb41dyQh6mKc  
oHqt3jRlxW5MDvf9QyIOR7VfFwK656es0UFilb74N9pRntzF1UgYzDGu3ppZVMdo  
lbxhm6dWS9OK/LfehKNT0OYI9aqk6F+U7cA6jxSC+iDBPXwdF4rs3KRyp3aQn6pj  
pp1yr7IB6Y4zv72Ee/PLZ/6rK6InC6WpK0nPV0YR7n9iDuPe1E4lxUMBH/T33+3h  
yuH3dvfgiWUOUkjdpMbyxX+XNle5uEliYBsi4lvbcTch8ruifCii5mDXkZrnMT8n  
wfYCV6v6kDdXkbgGRLKsR4pucbJtbKqlKUGxuZl2t7pfewKRc5nWecvDBZF3+1M  
pA8CAwEAAaOCAU8wggFLMB0GA1UdDgQWBBrVdE+yck/1YLpQ0dfmUVyaAYca1zAf  
BgNVHSMEGDAWgBQD3IA1VtFMu2bwo+lbG8OXsj3RVTAOBgNVHQ8BAf8EBAMCAYYw  
HQYDVROlBBYwFAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBHMCMBlGA1UdEwEB/wQIMAYBAf8C  
AQAwNAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBzABhhodHRwOi8vb2Nzc5kaWdp  
Y2VydC5jb20wYyZSBEViBUTFMgQ0EgLSBHMTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALPeP6wkb41dyQh6mKc  
oHqt3jRlxW5MDvf9QyIOR7VfFwK656es0UFilb74N9pRntzF1UgYzDGu3ppZVMdo  
lbxhm6dWS9OK/LfehKNT0OYI9aqk6F+U7cA6jxSC+iDBPXwdF4rs3KRyp3aQn6pj  
pp1yr7IB6Y4zv72Ee/PLZ/6rK6InC6WpK0nPV0YR7n9iDuPe1E4lxUMBH/T33+3h  
yuH3dvfgiWUOUkjdpMbyxX+XNle5uEliYBsi4lvbcTch8ruifCii5mDXkZrnMT8n  
wfYCV6v6kDdXkbgGRLKsR4pucbJtbKqlKUGxuZl2t7pfewKRc5nWecvDBZF3+1M  
pA8CAwEAAaOCAU8wggFLMB0GA1UdDgQWBBrVdE+yck/1YLpQ0dfmUVyaAYca1zAf  
BgNVHSMEGDAWgBQD3IA1VtFMu2bwo+lbG8OXsj3RVTAOBgNVHQ8BAf8EBAMCAYYw  
HQYDVROlBBYwFAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBHMCMBlGA1UdEwEB/wQIMAYBAf8C  
AQAwNAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBzABhhodHRwOi8vb2Nzc5kaWdp  
Y2VydC5jb20wYyZSBEViBUTFMgQ0EgLSBHMTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALPeP6wkb41dyQh6mKc  
oHqt3jRlxW5MDvf9QyIOR7VfFwK656es0UFilb74N9pRntzF1UgYzDGu3ppZVMdo  
lbxhm6dWS9OK/LfehKNT0OYI9aqk6F+U7cA6jxSC+iDBPXwdF4rs3KRyp3aQn6pj  
pp1yr7IB6Y4zv72Ee/PLZ/6rK6InC6WpK0nPV0YR7n9iDuPe1E4lxUMBH/T33+3h  
yuH3dvfgiWUOUkjdpMbyxX+XNle5uEliYBsi4lvbcTch8ruifCii5mDXkZrnMT8n  
wfYCV6v6kDdXkbgGRLKsR4pucbJtbKqlKUGxuZl2t7pfewKRc5nWecvDBZF3+1M  
pA8CAwEAAaOCAU8wggFLMB0GA1UdDgQWBBrVdE+yck/1YLpQ0dfmUVyaAYca1zAf  
BgNVHSMEGDAWgBQD3IA1VtFMu2bwo+lbG8OXsj3RVTAOBgNVHQ8BAf8EBAMCAYYw  
HQYDVROlBBYwFAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBHMCMBlGA1UdEwEB/wQIMAYBAf8C  
AQAwNAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBzABhhodHRwOi8vb2Nzc5kaWdp  
Y2VydC5jb20wYyZSBEViBUTFMgQ0EgLSBHMTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALPeP6wkb41dyQh6mKc  
oHqt3jRlxW5MDvf9QyIOR7VfFwK656es0UFilb74N9pRntzF1UgYzDGu3ppZVMdo  
lbxhm6dWS9OK/LfehKNT0OYI9aqk6F+U7cA6jxSC+iDBPXwdF4rs3KRyp3aQn6pj  
pp1yr7IB6Y4zv72Ee/PLZ/6rK6InC6WpK0nPV0YR7n9iDuPe1E4lxUMBH/T33+3h  
yuH3dvfgiWUOUkjdpMbyxX+XNle5uEliYBsi4lvbcTch8ruifCii5mDXkZrnMT8n  
wfYCV6v6kDdXkbgGRLKsR4pucbJtbKqlKUGxuZl2t7pfewKRc5nWecvDBZF3+1M  
pA8CAwEAAaOCAU8wggFLMB0GA1UdDgQWBBrVdE+yck/1YLpQ0dfmUVyaAYca1zAf  
BgNVHSMEGDAWgBQD3IA1VtFMu2bwo+lbG8OXsj3RVTAOBgNVHQ8BAf8EBAMCAYYw  
HQYDVROlBBYwFAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBHMCMBlGA1UdEwEB/wQIMAYBAf8C  
AQAwNAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBwEBBzABhhodHRwOi8vb2Nzc5kaWdp  
Y2VydC5jb20wYyZSBEViBUTFMgQ0EgLSBHMTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALPeP6wkb41dyQh6mKc  
oHqt3jRlxW5MDvf9QyIOR7VfFwK656es0UFilb74N9pRntzF1UgYzDGu3ppZVMdo  
lbxhm6dWS9OK/LfehKNT0OYI9aqk6F+U7cA6jxSC+iDBPXwdF4rs3KRyp3aQn6pj  
pp1yr7IB6Y4zv72Ee/PLZ/6rK6InC6WpK0nPV0YR7n9iDuPe1E4lxUMBH/T33+3h  
yuH3dvfgiWUOUkjdpMbyxX+XNle5uEliYBsi4lvbcTch8ruifCii5mDXkZrnMT8n  
wfYCV6v6kDdXkbgGRLKsR4pucbJtbKqlKUGxuZl2t7pfewKRc5nWecvDBZF3+1M  
pA8CAwEAAaOCAU8wggFLMB0GA1UdDgQWBBrVdE+yck/1YLpQ0dfmUVya
```

```
MIIMWwBFLmfKj/AHNHfZihwPGOc7w6UHcBZXH5RFZJNnww+WnKuTPI0HfnVH8lg==
-----END CERTIFICATE-----",
  "type": "server",
  "create_time": "2019-03-03 16:32:30",
  "private_key": "-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAUw5UDKAL8ij0el9XyoYtCg3RnrGzFujWVv+336Y/V6wdyggq
pccyOFZh/T57b665SyTxqJYC6g2WXOMym1JJqsWNVxbxg7ONXKCs3bXPSINtXLSuPM
H3rJ5Oa+dgN8lOdkdSZUhwzoYg4Rzksaozs3Nhq3i6wclihVGgLnuaq058jG80Gkj
7a0wJkrFEWChHiekdwOicKJDoMvVUruNbn0ihZDMcCsRAs58y304aglob2KMW7
E8qJW+o8KcOB+r3ESBHBQLPFAKVkaBCo8u3jj91FjtOrfjDr14a5cRKiD5v65c
BND5LZzpvQ4AwN2G98U/zLU9lUUnwiUB4CHLHQIDAQABAolBAGS5rISompP2OwA8
virwVRVXdPUQ5oxvbuTPys+A59RxVIU8kFW+qJ4fJMYsOfRXLtOtq+5tk20YBru
1ZLVfVqAowrELXB/J2ID+WTMkLORLSNlq1kW+nC9LL6PDY98LW/n7Fo5FskGI5HT
AxFGNGUvpr2vlojuL6nGfmcM47uscd9aP6ljxr4p70dhPVJzBdnMnXyWRk83dzt/
EOB/p8J5i3oo5Rucv4DOFb+01wXGAVyx5/zce+NZdhyrivkj3hHV55SxGhVWzWhj
a3dAlbpKwYgflJ0inRdJYmIjBdbGb2HFix7+ncBg8B2oerJXC6/fANwRGU5/LZU
5xuPVWkCgYEA6an8TY1unlGLYL5aBJ16Tx4usqMyTXr/T4zkQyftRPMt+ZuxVQHL
GHsg7XvLUSNd04MBZxtKZXAyVcpOm7OUYcl0i9ZAKWXXoXcBtn1Oom3gz/7RjAUnp
k+myxqCUSQ2J5z4u3Q8tyPVyNyBFXrKqdKfcYg85+yQVHBNMVrdvMCgYEAvd0C
hFpm83ha+VQp+9XN1DYZNUyqhibj/E3X9jAn+gDbzLKxw/D9en2RlIQYUrl8+iI8
QKk4cFoxyStQfxptz8QBpVeLajDN67zJ0Rk8AB50HHHcNSU8uFkaO8KxsvjBLS
+JltqfIAEraXLinbp1Fxcg9DSqDm6cw2DmrWa8CgYEA1UjIOUzo80i4HYWDC4Vn
OEK3o22do+WqmEvsfSG9BH5HedGvE7V3EO/6aY+1/ZXBDPvH8mRAs9v8lbeXow7
hWCiYZfB5jre8HyOU4l8dPUCmdxhrl913rRluAASqBlet32ztXuCNWzp1X4nBj
/yF3UqFQKZ7SihcDAZVwo4sCgYEAj7al/BcNzlcynX2mldhdh583b4/Ll+YCNm2Z
5eDHscZKmx8fLcjRpZE8dXagPqXmwtj6E1vDvQWP9m06VDNcThFHB+nO0tLmidSk
evmbScuiaTRmmbjZlTHY0hIqNsc7PgKF2DTklstEr0hLDFE826FN60PiDfMcbbd
Ax6L5EMcgYEA0+qhuQftKQKgdBXX9r3H8N0Tvh27ByfL3kKVYyOdUJMvsOQA6d97
8mEHYhrYt88f1sFpM7G09XpCmCBXwiKxw8+CDT9auD4r1snBnlLpqMPmanF4UDXH
L7s+4it+nIQy24P6g1PihtzMs+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_2b824c8bbe419992fb7974b2911c72",
  "certificate": "-----BEGIN CERTIFICATE-----
MIIDpTCCAo2gAwIBAgIUAKdmmOBYnFvoMAOGCSqGSIb3DQEBCwUAMGKxCzAJBgNV
BAYTAneh4MQswCQYDVQQLIDAJ4eDELMAKGA1UEBwwCeHgxCAZBgNVBAoMANh4MQsw
CQYDVQQLDAJ4eDELMAKGA1UEAwwCeHgxGTAXBgkqhkiG9w0BCQEWCnh4QDE2My5j
b20wHhcNMTCxMjA0MDM0MjQ5WWhcNMjA0MjA0MDM0MjQ5WjBpMQswCQYDVQGEWwI4
eDELMAKGA1UECAwCeHgxCAZBgNVBACMANh4MQswCQYDVQKDAJ4eDELMAKGA1UE
CwweHgxCAZBgNVBAMMANh4MRkwFwYJKoZIhvcNAQkBFgq4EeAxiNjMuY29tMIIB
ljANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCGKCAQEAwZ5UJULajWr7p6FVwGRQRjFN
2s8tZ/6LC3X82fajpVsYqF1xqEuUDndDXVD09E4u83MS6HO6a3blVQDP6/klNylD
iE6Vp8HH5BSKaCwKvG8lGWg1UM9wZfNryi14KgmpIFmCu9nA8yV/6MZAE6RSdmb
3iyNBmiZ8aZhGw2pl1Ywr+15MVqFGB+7ExkziROI7L8CfYCezKt/ooOvQsH1dz
Q8z1JXWdg8/9Zx7KtvgwU5PQM3cltSHX6lBPokMU8Z8TugLlTqQXKZOEgwajwQ5
mf2DPkVgM08XAgalJcligWd513koAdtUd5v+9irw+5LAuO3JclqTwvy7u/YwwlD
AQABo1AwTjAdBgNVHQ4EFgQUo5A2tlu+bcUfvGTD7wmEkhXKFjcwHwYDVR0JBgww
FoAUo5A2tlu+bcUfvGTD7wmEkhXKFjcwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0B
AQsFAAOCAQEAUWJ2rS6Mvlqk3GfEpbuez2j3X7l1z8Sxoqq6ntwB+rezvK3mc9H0
83qsVeUcoH+0AOLSHyFNM4FvRQL6X1hEheHarYwJK4agb231vb5erasuGO463eYEG
r4SftUm075yiV2xxbaBKrXJtpBp4WLL/s+LF+nklKjaOxkxmUX0sM4CTA7uFJypY
c8Tdr8lDDNqoUtMD8BrUCji+7lmMXRcC3Qi3oZJW76ja+kZASmKVPFD1ATih8TbA
i34R7EQDtFeiSvBdeKRSPp8c0KT8H1B4IXNkkCQs2WX5p4lm99+ZtLD4glw8x6lc
i1YhgnQbn5E0hz55OLu5jvOkKQjPCW+8Kg==
-----END CERTIFICATE-----",
  "type": "server",
  "create_time": "2018-09-28 03:00:47",
  "private_key": "-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAwZ5UJULajWr7p6FVwGRQRjFN2s8tZ/6LC3X82fajpVsYqF1x
qEuUDndDXVD09E4u83MS6HO6a3blVQDP6/klNylDiE6Vp8HH5BSKaCwKvG8lGWg1

```

```
UM9wZFnlryi14KgmpIFmcu9nA8yV/6MZAe6RSDmb3iyNBmiZ8aZhGw2p1YwR+15
MVqFFGB+7ExkziROi7L8CFCyCezK2/oOOvQsH1dzQ8z1JXWdg8/9Zx7Ktvgwu5PQ
M3cItSHX6iBPOkMU8Z8TugLITqQXKZOEGwajwvQ5mf2DPkVgM08XAgALJcLigWd5
13koAdtId5v+9irw+5LAuO3JclqwTvwy7u/YwwIDAQABAoIBACU9S5fjD9/jTMAXA
DRs08A+gGgZUxLn0xk+NAPX3LyB1tfdkCaFB8BccLzO6h3KZuwQOBPv6jkdvEDbx
Nwyw3eA/9GJslvKiHc0rejdvypymaw9I8MA7NbXHajrY7KpqDQyk6sx+aUTcy5jg
iMXLWdwXYHhJ/1HVOo603oZyiS6HZeYU089NDUcX+1Sji3e5Ke0gPVXEgCq1O11/
rh24bMxnwZo4PKBWdcMBN5Zf/4ij9vrZE+fFzW7vGBO48A5lvZxWU2U5t/OZQRtN
1uLOHmMFa0FIF2aWbTVfwdUWAFsvAOKHj9V8BXOUwKOUuEktdkfAlvrmsFrO/H
yDeYYPkCgYEA/S55CBbR0sMXpSZ56uRn8JHApZJhgkgvYr+FqDUq/e92nAzf01P
RoEBUajwrnf1ycevN/SDfbtWzq2XJGqhWdJmtpO16b7KBsC6BdRcH6dnOYh31jgA
vABMIP3wzI4zSVTyxRE8LDuboytF1mSCeV5tHYPQTZNwrplDnLQhywcGgYEAw8Yc
Uk/eiFr3hfH/ZohMfV5p82Qp7DNIGRzw8YtVG/3+vNXrAXW1VhugNhQY6L+zLzJC
aKn84ooup0m3YCG0hvlNqluvzfsuzQgtjTXyaE0cEwsjUusOmiuj09vVx/3U7siK
Hdj2ICPCvQ6Q8tdi8jV320gMs05AtaBkZdsiWUCgYEAtLw4Kk4f+xTKDFsrLUNf
75wcqhWVBiwBp7yQ7UX4EysJPKZcHMRTk0EEcAbpyaJZE3I44vjp5ReXIHNLMfPs
uvl34J4Rfot0LN3n7cFrAi2+wpNo+MOBwrNzpRmijGP2uKKrq4JiMjFbKV/6utGF
Up7Vxfws904JYpqGaZctiECgYA1A6nZtF0riY6ry/uAdXpZHL8ONNqRZtWoT0kD
79otSVu5iSiRbaGcXsDExC52oKrSDAgFtbqQUiEOFG09UcXfoR6HwRkba2CiDwve
yHQLQI5Qrdxz8Mk0glrNrSM4FamcW9vi9z4kCbQyoC5C+4gqeUURpDlkQBWP2Y4
2ct/bQKBgHv8qCsQTZphOxc31BJPa2xVhuv18cEU3XLURVfUZ/1f43JhLp7gynS2
ep++LKUi9D0VGXY8bqvJjBECeCo85vl8NpCXwe/LoVoln+7KaVIZMwqoGMfgNl
nEqm7HWkNxxHh8A6En/ljleuddS1sf9e/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 <i>YYYY-MM-DDTHH:MM:SS</i> format.
create_time	String	Specifies the time when the certificate was created. The UTC time is in <i>YYYY-MM-DDTHH:MM:SS</i> format.
update_time	String	Specifies the time when the certificate was updated. The UTC time is in <i>YYYY-MM-DDTHH:MM:SS</i> 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-----
\nMIIC4TCCAcmgAwIBAgICERewDQYJKoZIhvcNAQELBQAwFzEVMBMGGA1UEAxMMTXID
\nb21wYW55IENBMBA4XDTE4MDcwMjEzMjU0N1oXDTQ1MTExNzEzMjU0N1owFDESMBAG
\nA1UEAwwJbG9jYWxob3N0MIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
\n0FQGzi3ucTX+DNud1p/b4XVM6I3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5
\nuU0nQPQZKUrZz3rQeLN9mYiUTJZPutYlFDDbB8CtIgV+eyU9yYJstWx/Bm5kWNPh9
\n7B9Yu9pbp2u6zDA99IC4ekKD93KuzxLnLmSle4Y3dbYwk0LpMDL6lfCHKt/W7jaS
\nlnlAzlsx+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylYKy4zgnv1tn/K
\nny09cxLKAftgoZWQD2FAZJf9F7k1kYNwqITz3CPILZUUn7yw3nkOOtLMl28IEv0WY
\nYd7CMJQkS1NPJBKNOGfr/wIDAQABozowODAhBgNVHREEGjAYggpkb21hW4uY29t
\nnhwQKuUvJhwR/AAABMBMGGA1UdJQMMAoGCCsGAQUFBwMBMA0GCsQGSQSIb3DQEB
\nCwUA\nA4IBAQA8lMQJxaTey7EjXtRLSVIEAMftAQPG6jijNQuvIBQYUDauDT4W2XU5wAn
\nnjiOyQ83va672K1G9s8n6xIH+xwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDa
\nnezmcCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNyjvPRLYlzp1HMnl6hkjPk4PCZ
\nnwkNha0dlScati9Cct3UzXSNOJSLaKdHErH08lqd+1BchScxCfk0xNItn1HZZGml
\nn+vbmunok3A2luc14rnrcbkGYqxGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZ
\nniYsGDVN+9QBd0eYUHce+77s96i3l
\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": "a31d2bdcf7604c0faadb058e1e08819",
  "admin_state_up": true,
  "name": "https_certificate",
  "private_key":
    "-----BEGIN PRIVATE KEY-----
\nMIIEvgIBADANBgkqhkiG9w0BAQEFAASCBAKgwggSkAgEAAoIBAQQDQVAbOLe5xNf4M
\n253Wn9vhdUzojetjv4J+B7kYwsMhRcgdcJ8KcN1nfzTvI2ksXITQ2o9BkpStnPe
\nntB4s32ZiJRMlk+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72Luna7rM
\nnMD30gLh6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8Icq39buNplgDOWzEP5AqzXt
\nnCOfYn6RTH5SRug4hKNN7sT1eYMsLHu7wtEBDKVgrLjOCe/W2f8rLT1zEsOAw2Chl
\nnZAPYUBkl/0XuTWRg3CohPPcl+UtlRSfvLDeeQ460swjbgwS/RbJh3slwlCRLU08k
\nnEo04Z9H/AgMBAAECggEAEleaQqHCWZk/HyYN0Am/GJSGFa2tD605XY2fUieh8/Hl
\nnfvCArftGgMaYWPNSNCJRMXB7tPwpQu19esjz4Z/cR2Je4fTLPrffGUshFgZjv5OQB
\nnZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr
\nnciu9YklnNEHu6uRJ5g/eGGX3KQynTvVIhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M
\nnEGpfYI6ADHlwFZcT/RNAXhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7Ale
\nnkrquPtfV1vWklg+bUFhgGaiAEYTpAUN9t2DVliijgQKBgQDnYMMsaF0r557CM1CT
\nnXUqgCZO8MKeV2jf2drlxRRwRL33SksQbzAQ/qRLd7GP3sCGqvkvxWY2FPdFYf8kx
\nnGcCeZPcleZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/fbwjpp7dt
\nnJ7n8EzkRUNE6alMHOFEeych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr
\nniWgTWHXPZxUQaYhjpXo6+IMl6DpExiDgBAkMzJGlV57yQiYWU+wthAr9urbWYdGZ
\nnIS6VjoTkF6r7VZolLX0fbuXh6lm8K8lQRfBpJff56p9phMwaBpDNDrfpHB5utBU
\nnxs40yldp6wKBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zJf3bGSXU/jR4eB
\nn1lVQhELGI9CbKSdzKM71GyElmix/T7FnJSHIWLho1qVo6AQyduNWnAQD15pr8KAd
\nnXGXAZZ1FQcb3KYa+2fflERmazedOTwJYZ0tGqZnXkEeMdSLkmlqLRigWhGQKBgDak
\nn/735uP20KKqhNehZpC2dJei7OilRhCS/dKASUXHSW4fptBnUxACYocdDxtY4Vha
\nnfl7FPMdvGl8ioYbvlHFh+X0Xs9r1S8yeWnHoXMB6eXWmYKMJRaoveLa+2cFm1Agf
\nn7nLhA4R4lqm9IpV6SKegDUkR4fxp9pPyodZPqBLA0GBAJkD4wHW54Pwd4Ctfk9o
\nnjHjWB7pQLUYpTZO9dm+4fPMn9Okf43AE2yAOaAP94GdzdDJkxfciXKcsYr9lluk
\nnfaoXgjkR7p1zERiWZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BUIGKMWXzuEd
\nn3fy+1rCUwzOp9LSjtYf4ege
\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: <code>www.test.com</code> • In addition to the requirements for common domain names, a wildcard domain name can start with an asterisk (*). Example: <code>*.test.com</code> 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 <i>YYYY-MM-DDTHH:MM:SS</i> format.
create_time	String	Specifies the time when the certificate was created. The UTC time is in <i>YYYY-MM-DDTHH:MM:SS</i> format.
update_time	String	Specifies the time when the certificate was updated. The UTC time is in <i>YYYY-MM-DDTHH:MM:SS</i> format.

Example Request

- Example request: Updating a certificate
PUT <https://{Endpoint}/v2.0/lbaas/certificates/23ef9aad4ecb463580476d324a6c71af>

```
{
  "certificate": "-----BEGIN CERTIFICATE-----
\nMIIC4TCCAcmgAwIBAgI CERewDQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMMTXID
\nb21wYW55IENBM4XDTE4MDcwMjEzMjU0N1oXDTQ1MTExNzEzMjU0N1owFDESMBAG
\nA1UEAwWJbG9jYWxob3N0MIIlBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
\n0FQGzi3ucTX+DNud1p/b4XVM6I3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5
\nU0NqPQZKUrZz3rQeLN9mYiUTJZPutYlFDDbB8CtIgV+eyU9yYJslWx/Bm5kWNPh9
\n7B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/W7jaS
\nnIAzlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylyKy4zgnv1tn/K
\nny09cxLKAftgoZWQD2FAZJf9F7k1kYNwqlTz3CPILZUUn7yw3nkOOTLMI28IEv0Wy
\nYd7CMJQkS1NPJBKNOGfR/wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29t
\nnhwQKUuvJhwr/AAABMBMGA1UdJQMMAoGCCsGAQUFBwMBMA0GCsGSIb3DQEBCwUA
\nA4IBAQA8IMQJxaTey7EjXtRLSVIEAMftAQPG6jijNQuvlBQYUDauDT4W2XUZ5WAn
\nnjiOyQ83va672K1G9s8n6xlH+xwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDa
\nnezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNyjvPRLYLzp1HMnl6hkjPk4PCZ
\nnwKnha0dlScati9Cct3UzXSNJOSLaKdHErH08lqd+1BchScxChk0xNITn1HZZGml
\nn+vbmunok3A2luc14rnsrbcGyqXGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/mZ
\nniYsGDVN+9QBd0eYUHce+77s96i3l
\n-----END CERTIFICATE-----",
  "description": "description for certificate",
  "domain": "www.elb.com",
  "name": "https_certificate",
  "private_key": "-----BEGIN PRIVATE KEY-----
\nMIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDQVAbOLe5xNf4M
\n253Wn9vhdUzojetjv4J+B7kYwsMhRcgdcj8KCnX1nfzTvl2KsXLTQ2o9BkpStnP
\nbtB4s32ZiJRmlk+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM
\nnMD30gHh6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8lCq39buNplgDOWzEP5AzsXt
\nnCOFYn6RTH5SRug4hKNN7sT1eYMSlHu7wtEBDKVgrLjOCe/W2f8rLT1zEsoAW2Chl
\nnZAPYUBkl/0XuTWRg3CohPPcl+UtlRSfvLDeeQ460swjbgwS/RbJh3slwLCRLU08k
\nnEo04Z9H/AgMBAAECggEAEleaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/Hl
\nnfvcArftGgMaYWPNSCJRMXB7tPwpQu19esjz4Z/cR2Je4fTLPrffGUSHFgZjv5OQB
\nnZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr
\nnciu9YklNNEHu6uRJ5g/eGGX3KQynTvVlhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M
\nnEGpfYl6AdHlwFZcT/RNAXhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7Ale
\nnkrgruPtFv1vWklg+bUfhgGaiAEYTpAUN9t2DVIijgQKBgQDnYMMsaF0r557CM1CT
\nnXUqgCZo8MKeV2jf2drlxRRwRL33SksQbzAQ/qrLdT7GP3sCGqvkvWY2FPdFyF8kx
\nnGcCeZPcleZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/fbwjpp7dt
\nnJ7n8EzkRUNE6alMHOFEeych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr
\nniWgTWHXPZxUQaYhpjXo6+IMl6DpExiDgBAkMzJGlvS7yQiYWU+wthAr9urbWYdGZ
\nnIS6VjoTkF6r7VZolLXX0fbuXh6lm8K8lQRfBpJff56p9phMwaBpDNDrfpHB5utBU
\nnxs40yldp6wKBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKscpAg38zJf3bGSXU/jr4eB
\nn1lVQhELGI9CbKsdzKM71GyElmix/T7FnSHIWIho1qVo6AQyduNWNnAQD15pr8KAd
\nnXGXAZZ1FQcb3KYa+2fIERmazdOTWjYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak
\nn/735uP20KKqhNehZpC2dJei7OilGRhCS/dKASUXHSW4fptBnUxACYocdDxtY4Vha
\nnfl7FPMdvGlbioYbvlHFh+X0Xs9r1S8yeWnHoXMB6eXWmYKMMJAoveLa+2cFm1Agf
\nn7nLhA4R4lqm9lpV6SKegDUK4fxp9pPyodZPqBLLAoGBAJKD4wHW54PwD4Ctfk9o
\nny09cxLKAftgoZWQD2FAZJf9F7k1kYNwqlTz3CPILZUUn7yw3nkOOTLMI28IEv0Wy
\nnfaoXgJkR7p1zERIwZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BUIGKMWXzuEd
\nn3fy+1rCUwzOp9LSjtYf4eje
\n-----END PRIVATE KEY-----"
}
```

Example Response

- Example response

```
{
  "certificate": "-----BEGIN CERTIFICATE-----
\nMIIC4TCCAcmgAwIBAgI CERewDQYJKoZIhvcNAQELBQAwFzEVMBMGA1UEAxMMMTXID
\nb21wYW55IENBM4XDTE4MDcwMjEzMjU0N1oXDTQ1MTExNzEzMjU0N1owFDESMBAG
\nA1UEAwWJbG9jYWxob3N0MIIlBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
\n0FQGzi3ucTX+DNud1p/
b4XVM6I3rY7+Cfge5GMLDIUXIHXCfCgp19Z3807yNpLF5\nU0NqPQZKUrZz3rQeLN9mYiUTJZPutYlFDDbB8CtIgV+eyU9yYJslWx/
Bm5kWNPh9\n7B9Yu9pbp2u6zDA99IC4ekKD93KuzxlnLmSle4Y3dbYwk0LpMDL6lfCHKt/W7jaS
\nnIAzlsxD+QM6l7QjhWJ+kUx+UkboOISjTe7E9XmDLJR7u8LRAQylyKy4zgnv1tn/K
\nny09cxLKAftgoZWQD2FAZJf9F7k1kYNwqlTz3CPILZUUn7yw3nkOOTLMI28IEv0Wy
\nYd7CMJQkS1NPJBKNOGfR/wIDAQABozowODAhBgNVHREEGjAYggpkb21haW4uY29t
\n-----END CERTIFICATE-----",
  "description": "description for certificate",
  "domain": "www.elb.com",
  "name": "https_certificate",
  "private_key": "-----BEGIN PRIVATE KEY-----
\nMIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDQVAbOLe5xNf4M
\n253Wn9vhdUzojetjv4J+B7kYwsMhRcgdcj8KCnX1nfzTvl2KsXLTQ2o9BkpStnP
\nbtB4s32ZiJRmlk+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM
\nnMD30gHh6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8lCq39buNplgDOWzEP5AzsXt
\nnCOFYn6RTH5SRug4hKNN7sT1eYMSlHu7wtEBDKVgrLjOCe/W2f8rLT1zEsoAW2Chl
\nnZAPYUBkl/0XuTWRg3CohPPcl+UtlRSfvLDeeQ460swjbgwS/RbJh3slwLCRLU08k
\nnEo04Z9H/AgMBAAECggEAEleaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/Hl
\nnfvcArftGgMaYWPNSCJRMXB7tPwpQu19esjz4Z/cR2Je4fTLPrffGUSHFgZjv5OQB
\nnZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr
\nnciu9YklNNEHu6uRJ5g/eGGX3KQynTvVlhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M
\nnEGpfYl6AdHlwFZcT/RNAXhP82lg2gUJSgAu66FfDjMwQXKbafKdP3zq4Up8a7Ale
\nnkrgruPtFv1vWklg+bUfhgGaiAEYTpAUN9t2DVIijgQKBgQDnYMMsaF0r557CM1CT
\nnXUqgCZo8MKeV2jf2drlxRRwRL33SksQbzAQ/qrLdT7GP3sCGqvkvWY2FPdFyF8kx
\nnGcCeZPcleZYCQAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/fbwjpp7dt
\nnJ7n8EzkRUNE6alMHOFEeych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr
\nniWgTWHXPZxUQaYhpjXo6+IMl6DpExiDgBAkMzJGlvS7yQiYWU+wthAr9urbWYdGZ
\nnIS6VjoTkF6r7VZolLXX0fbuXh6lm8K8lQRfBpJff56p9phMwaBpDNDrfpHB5utBU
\nnxs40yldp6wKBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKscpAg38zJf3bGSXU/jr4eB
\nn1lVQhELGI9CbKsdzKM71GyElmix/T7FnSHIWIho1qVo6AQyduNWNnAQD15pr8KAd
\nnXGXAZZ1FQcb3KYa+2fIERmazdOTWjYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak
\nn/735uP20KKqhNehZpC2dJei7OilGRhCS/dKASUXHSW4fptBnUxACYocdDxtY4Vha
\nnfl7FPMdvGlbioYbvlHFh+X0Xs9r1S8yeWnHoXMB6eXWmYKMMJAoveLa+2cFm1Agf
\nn7nLhA4R4lqm9lpV6SKegDUK4fxp9pPyodZPqBLLAoGBAJKD4wHW54PwD4Ctfk9o
\nny09cxLKAftgoZWQD2FAZJf9F7k1kYNwqlTz3CPILZUUn7yw3nkOOTLMI28IEv0Wy
\nnfaoXgJkR7p1zERIwZuFF63SB4aiyX1H7IX0MwHDZQO38a5gZaOm/BUIGKMWXzuEd
\nn3fy+1rCUwzOp9LSjtYf4eje
\n-----END PRIVATE KEY-----"
}
```

```
\nhwQKuUvJhwr/AAABMBMGA1UdJQMMMAoGCCsGAQUFBwMBMA0GCsGSIb3DQEBCwUA
\nA4IBAQA8IMQxaTey7EjXtRLSVIEAMftAQPG6jjNQvIBQYUDauDT4W2XU25wAn
\njiOyQ83va672K1G9s8n6xLH+xwwdSNnozaKzC87vwSeZKIOdl9I5I98TGKI6OoDa
\nnezmzCwQYtHBMVQ4c7Ml8554Ft1mWSt4dMAK2rzNYjvPRLYLzp1HMnl6hkjPk4PCZ
\nnwKnha0dlScati9Cct3UzXSNJOSLaKdHErH08lqd+1BchScxCfk0xNITn1HZZGml\n
+vbmunok3A2lucl14nrsrckbGYqXGikySN6B2cRLBDK4Y3wChiW6NVYtVqcx5/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-----
\nMIIEvGlBADANBgkqhkiG9w0BAQEFAASCBAKgwggSkAgEAAoIBAQDQVAbOLe5Xnf4M
\n253Wn9vhdUzojetjv4j+B7kYwsMhRcgdcJ8KcnX1nfzTvl2ksXLTQ2o9BkpStnP
\nB4s32ZiJRMlk+61iUUMNsHwK2WBX57JT3JgmyVbH8GbmRY0+H3sH1i72luna7rM
\nMD30gLh6QoP3cq7PGWcuZKV7hjd1tjCTQukwMvqV8lq39buNpIgDOWZEP5AqXt
\nCOFYn6RTH5SRug4hKNN7sT1eYMsLHu7wtEBDKVgrLjOCe/W2f8rLT1zEsoAW2Chl
\nZAPYUBkl/0XuTWRg3CohPPcl+UtlRSfvLDeeQ460swjbgwS/RbJh3slwCRLU08k
\nEo04Z9H/AgMBAAECggEAEleaQqHCWZk/HyYN0Am/GJSGFa2tD60SXY2fUieh8/Hl
\nfvCArftGgMaYWPSPNCJRMXB7tPwpQu19esjz4Z/cR2Je4fTLPrffGUshFgZjv5QOB
\nZVe4a5Hj1OcgJYhwCqPs2d9i2wToYNBbcfgh8lSETq8YaXngBO6vES9LMhHkNKKr
\nnciu9YkInNEHu6uRI5g/eGGX3KQynTvVlhnOVGAJvjTXcoU6fm7gYdHAD6jk9lc9M
\nEGpfYl6AdHlwFZcT/RNAXhP82lg2gUJSgAu66FFdJmWQXKbafKdP3zq4Up8a7Ale
\nnkrguPtFv1vWklg+bUFhgGaiAEYTpAUN9t2DVliijgQKBgQDnYMMsaF0r557CM1CT
\nXUqgCZ08MKeV2jf2drLxRRwRL33SksQbzAQ/qRLdT7GP3sCGqvkxWY2FPdFYf8kx
\nGcCeZPcleZYQCAM41pjtsaM8tVbLWVR8UtGBuQoPSph7JNF3Tm/JH/fbwjpp7dt
\nJ7n8EzkRUNE6aIMHOFEEych/PQKBgQDmf1bMogx63rTcwQ0PEZ9Vt7mTgKYK4aLr
\nniWgTWHXPZxUQaYhpxo6+IMl6DpExiDgBAkMzJGlvS7yQiYWU+wthAr9urbWYdGZ
\nlS6VjoTkF6r7VZolLXX0fbuXh6lm8K8lQRfBpjff56p9phMwaBpDNDrfpHB5utBU
\nxs40yldp6wKBgQC69Cp/xUwTX7GdxQzEJctYiKnBHKcspAg38zf3bGSXU/jR4eB
\nlIVQhELG9CbKsdzKM71GyElmix/T7FnJSHIWIho1qVo6AQyduNWnAQD15prKAd
\nXGXAzz1FQcb3KYa+2fflERmazdOTWjYZ0tGqZnXkEeMdSLkmqlCRigWhGQKBgDak
\n/735uP20KKqhNehZpC2dJei7OilgRhCS/dKASUXHSW4fptBnUxACYocdDxtY4Vha
\nnfl7FPMdvGl8ioYbvlHFh+X0Xs9r1S8yeWnHoXMB6eXWmYKMrAoveLa+2cFm1Agf
\n7nLhA4R4lqm9lpV6SKegDUkR4fxp9pPyodZPqBLLAoGBAJkD4wHW54PwD4Ctfk9o
\nnjHjWB7pQLUYpTZO9dm+4fpCMn9Okf43AE2yAOaAP94GdzdDlKxfciXKcsYrIluk
\nnfaoXgjkR7p1zERiWZuFF63SB4iayX1H7IX0MwHDZQO38a5gZaOm/BUIGKMWXzuEd
\n3fy+1rCUwzOp9LSjtYf4ege
\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	<i>Dictionary data structure</i>	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

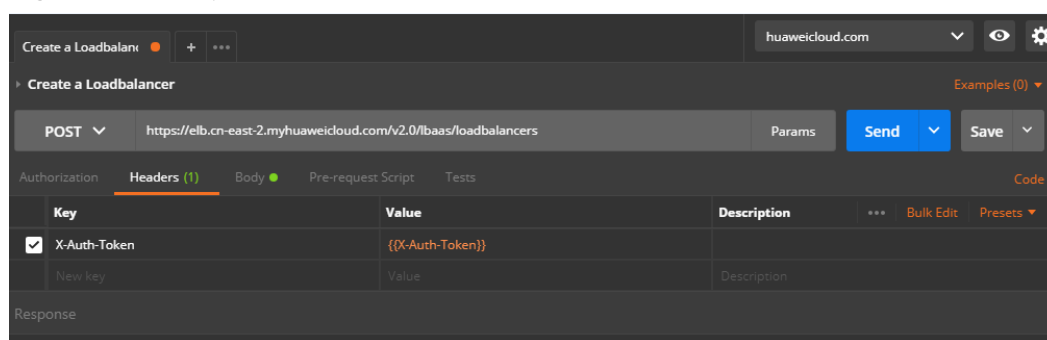
Method	URI	Description
POST	/v2.0/lbaas/loadbalancers	Creates a load balancer.

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

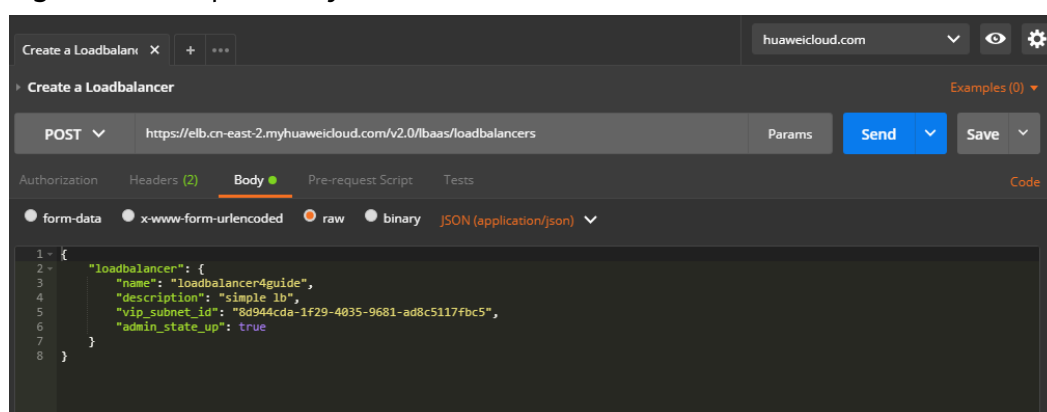


NOTE

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

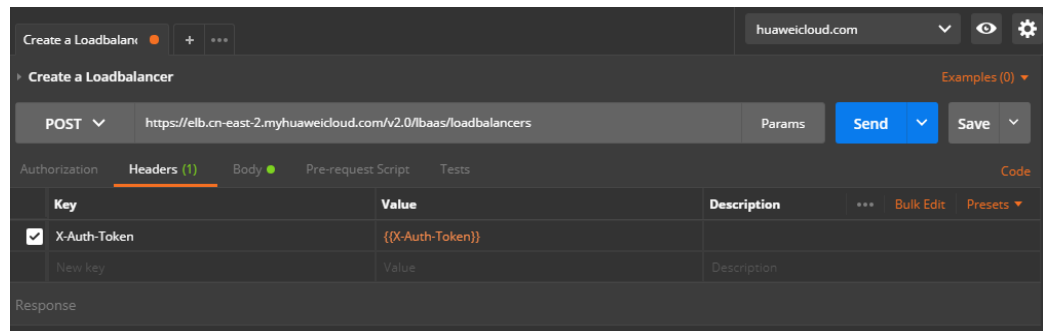
API Format

Method	URI	Description
POST	/v1/{tenant_id}/publicips	Applies for an EIP.

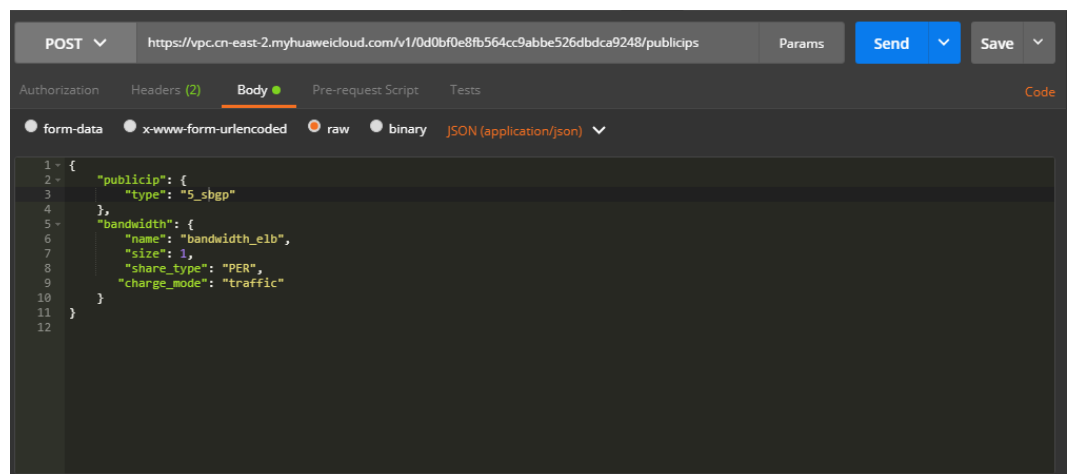
Procedure

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*.

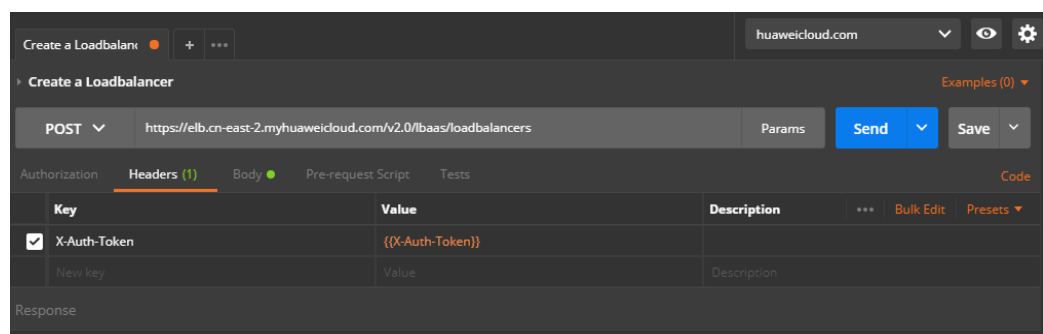
Bind the EIP

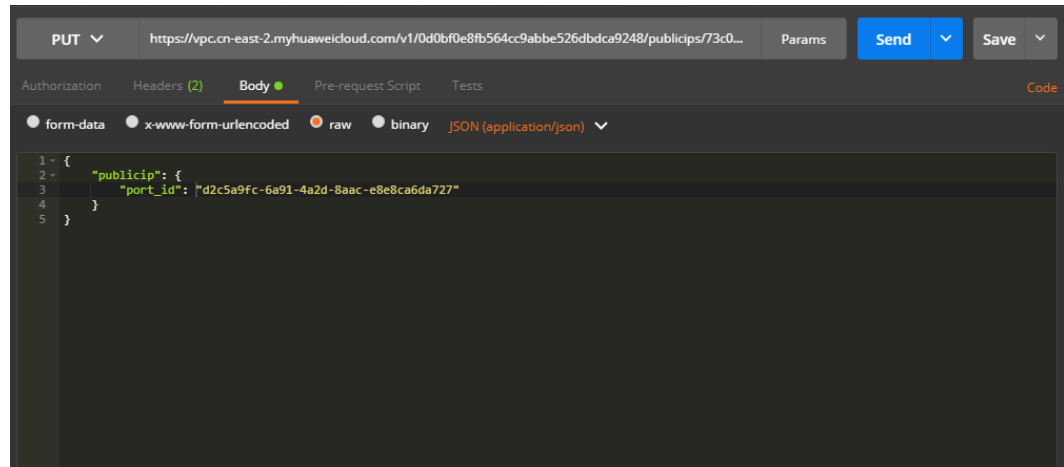
API Format

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

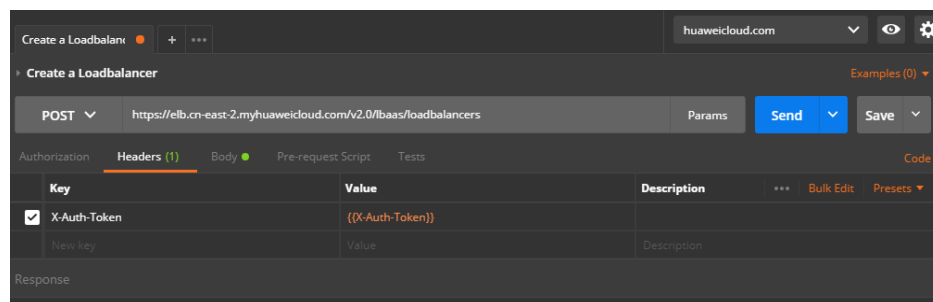
Method	URI	Description
POST	/v2.0/lbaas/listeners	Adds a listener.

Constraints

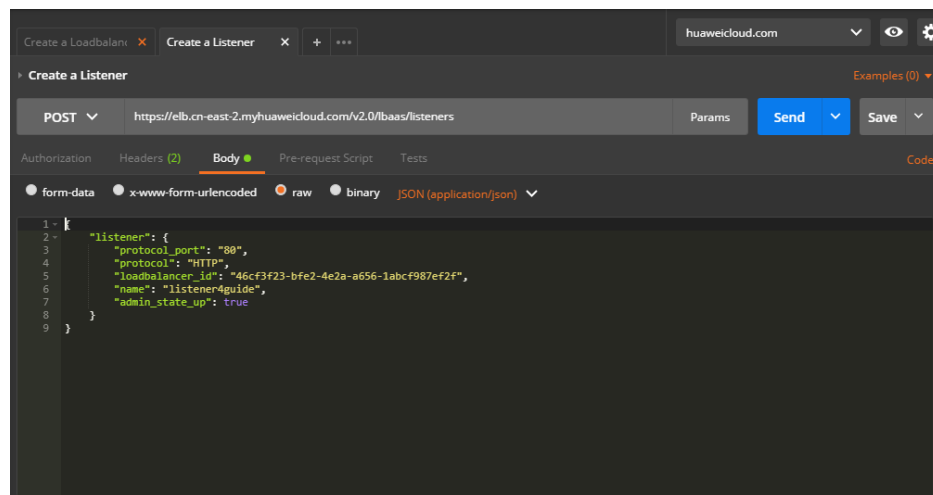
Each listener added a load balancer can listen on only one port.

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
  }
}
```

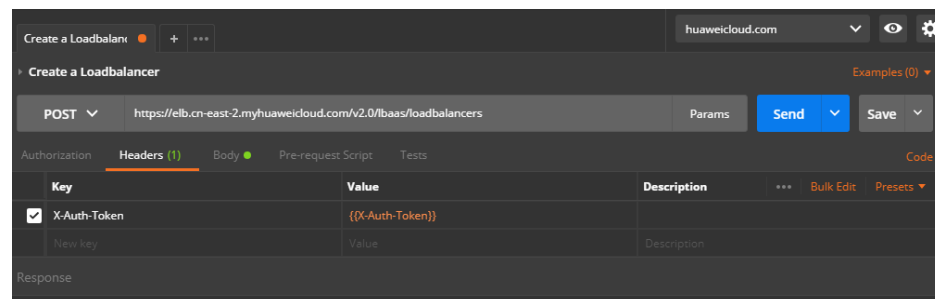
10.4.6 Creating a Backend Server Group

API Format

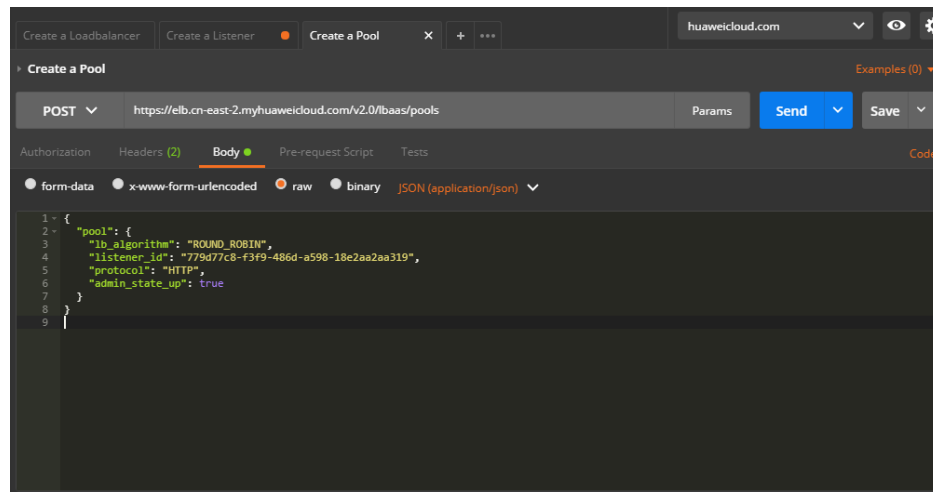
Method	URI	Description
POST	/v2.0/lbaas/pools	Adds a backend server group.

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

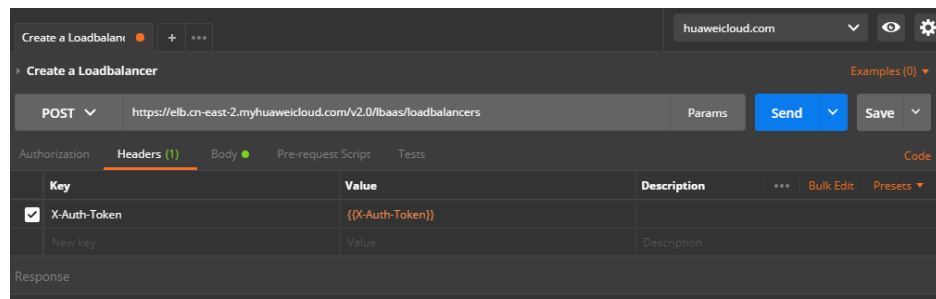
Method	URI	Description
POST	/v2.0/lbaas/pools/{pool_id}/members	Adds backend servers that belong to a backend server group.

Constraints

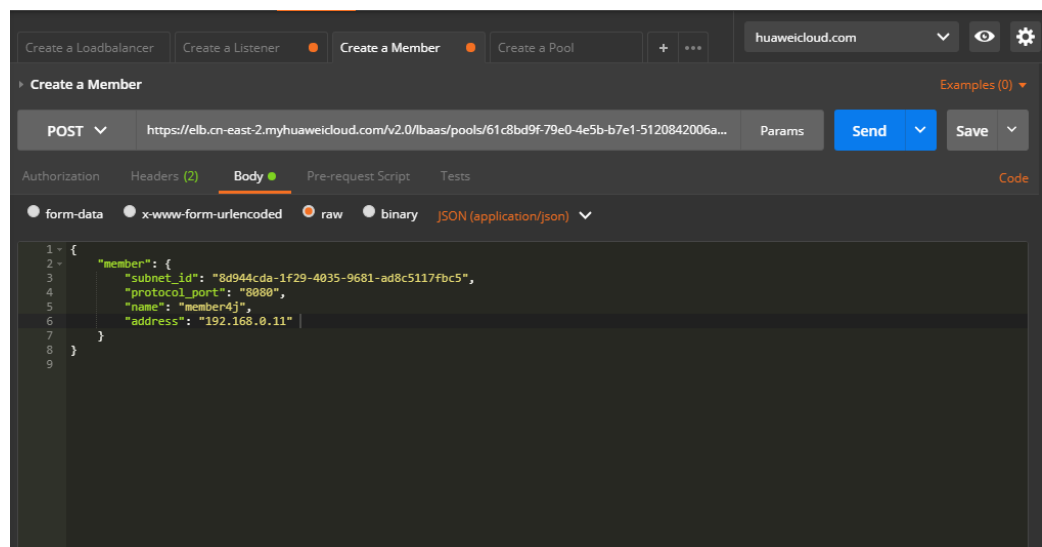
- Two backend servers in the same backend server group must have different IP addresses and ports.
- The subnet specified during server creation and the subnet to which the virtual IP address belongs must be in the same VPC.
- The value of **admin_state_up** must be **true**.

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": "0d0bf0e8fb564cc9abb526dbdca9248",  
    "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

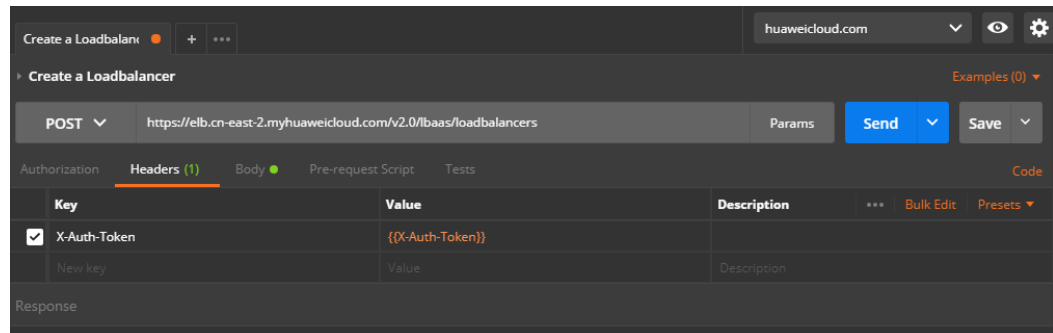
Method	URI	Description
POST	/v2.0/lbaas/ healthmonitors	Configures a health check.

Constraints

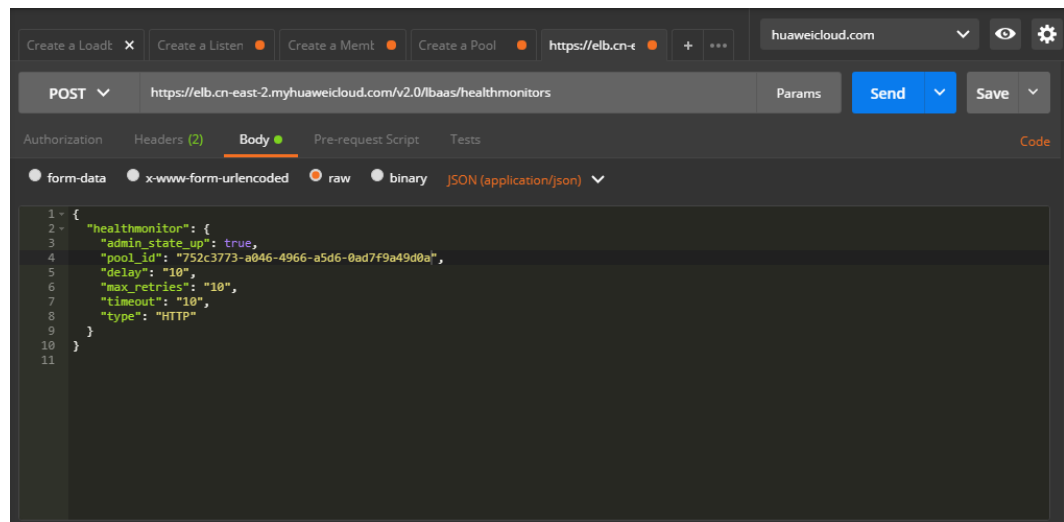
- The security group must have rules to allow access from the 100.125.0.0/16 network segment.
- The value of **admin_state_up** must be **true**.
- To use UDP for health checks, the backend server group must use UDP as backend protocol.

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.

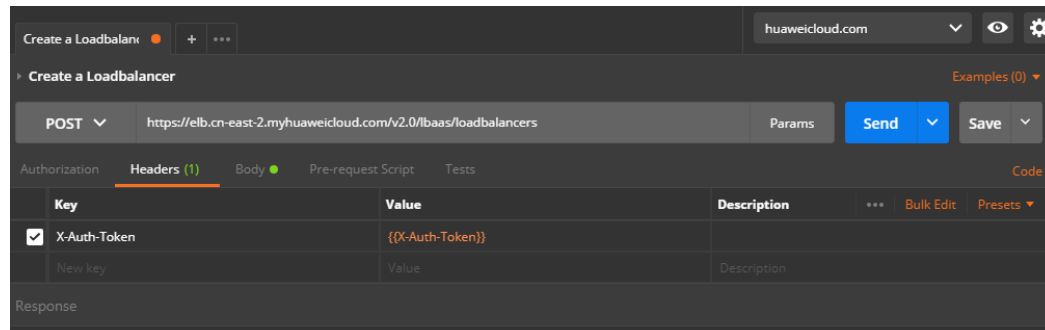
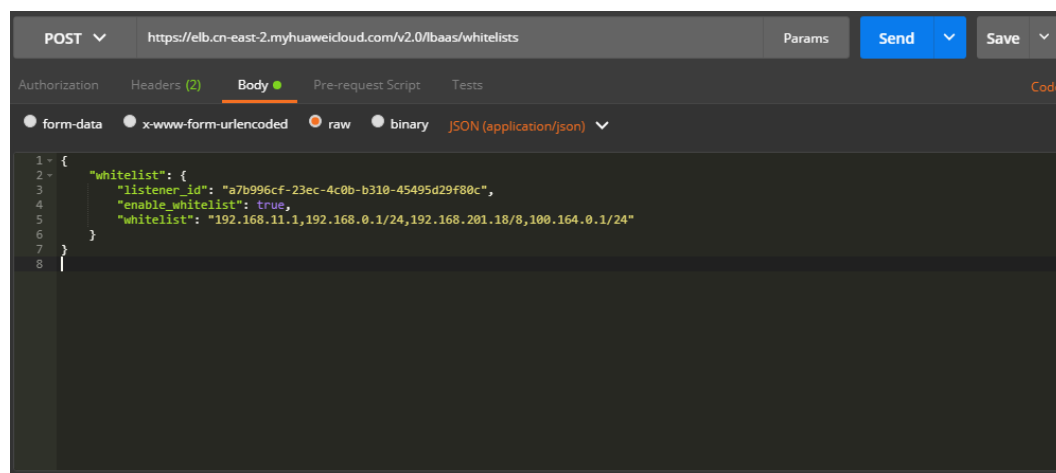
----End

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

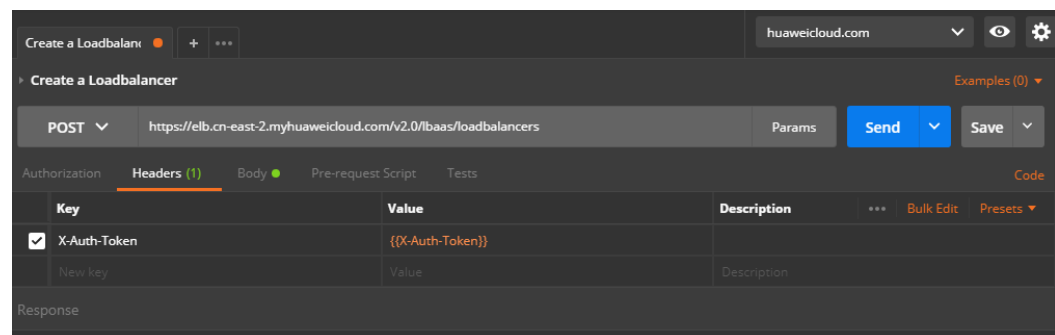
Request body in [Step 2](#)

```
{
  "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.

[illegible]

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
\nqEuUDndDXVD09E4eA4z8M56HO6a3blVQDp6/
klnYldiE6Vp8HH5BSKaCWKVg8lGWg1\nUM9WZFnlryi14KgmpIFmcu9nA8yV/
6MZAE6RSDmb3iyNBmiZ8aZhGw2pl1YwR+15\nMVqFFGB+7ExkziROi7L8CFCyCezK2/
oOOvQsH1dzQ8z1JXWdg8/9Zx7Ktvgwu5PQ
\nM3ctSHX56iBPOMU8Z8TwwGLITqQXXKOEGwajwvQ5mf2DPkvM08XAgALJcLigwD5\n1n3koAdtUd5v+9irw
+5LAuoQ3JclqwTvwy7u/YwUlDAQABaoIBACU9S5fjD9/jTMXA\nnDRsO8A+gGgZUXLn0xk
+NAPX3LyB1tfdkCaFB8BccLzO6h3KZuwQOBpv6jkdvEDbx\nnNwyw3eA/
9GSjlviKHc0rejdyvPyaw9I8MA7NbXHaJRy7KpqDQyk6sx+aUTcy5jg\nniMXLWdwXYHhJ/
1HVo0603oZYi56HZeyU089NDUCx+1SJi3e5Ke0gPVXEQCq1O11/\nnrh24bMxnwZo4PKBWdcMBN5Zf/4ij9vrZE
+ffZw7vGBO48A5lvZXWU2U5t/UZOZRtN
\n1uLOHmMQw0FIFF2aWBTVfwUWAFsvAoKHj9VV8BXOUwKOUuektkdfAlvrmsFrO/H\nnyDeYYpkCgYE/
S55CBbR0sMXpSZ56uRn8JHApZJhgkgvYr+FqDUUq/e92nAzf01P\nnRoEBUajwrnf1ycevN/
SDfbtWzq2XJGqhWdJmtpO16b7KBsC6BdRcH6dnOYh31jgA
\nnvABMIP3wzl4zSVTyxRE8LDuboytF1mScEv5tHYPPQTZNwrplDnLQhywcCgYEAw8Yc\nnUK/eiFr3hfH/
ZohMfv5p82Qp7DNIGRzw8ytVG/3+vNXrAXW1VhugNhQY6L+zLTJC
\nnaKn84ooop0m3YCg0hvlNqJuvfsuzQgtjTXyaEOcEwsjUusOmuiuj09vVx/3U7siK
\nnHdj2ICPCvQ6Q8tdi8vj320gMs05AtaBkZdsiWUCgYEAAtLw4Kk4fx+tTKDFsrLUNf
\nn75wqcqhWVBiwBp7yQ7UX4EYSJKZCHMRtk0EEcAbpyajZE3l44vp5ReXIHNLMFPs
\nnuvl34J4Rfor0tLN3n7cFAi2+wpNo+MOBwrNzpRmijGP2uKKrq4JImJfBKv/6utGF
\nUp7VxfwS904JypqGaZctilECgYA1A6nZtF0riY6ry/uAdXPZHLSOHNNqRztWoT0kd
\nn79otVSu5IisRbaGCxsDexC52oKrSDAGftbqQUiEOFG09UcXfoR6hwRkba2CiDvwve
\nnyHQLQI5Qrdxz8Mk0glrNrSM4FAMcW9vi9z4kCbQyoC5C+4qqeUUURpDIkBWP2Y4\nn2ct/
bQKBGhv8qCsQQTZphOxc31BJPa2xVhuv18cEU3XLUrVFUZ/1f43JhlP7gynS2\nnep+
+LKUi9D0VGXY8bqvJfJBECoeu85vl8nPcxwe/LoVoln+7KaVIZMwqoGMgfNI\nnnEqm7HWKNxHhf8A6En/
JleuddS1sf9e/x+TJN1Xhnt9W6fe7Fk1\nn-----END RSA PRIVATE KEY-----",
  "id": "e3c066329baa4a90bfbe13ec3d3cb8c",
  "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
\nBAYTAnh4MQswCQYDVQQLDAJ4eDELMAkGA1UEBwwCeHgxGzAJBgNVBAAoManh4MQsw
\nCQYDVQQLDAJ4eDELMAkGA1UEAwwCeHgxGTAXBgkqhkiG9w0BQCQEWCh4QDE2My5j
\nb20wHhcNMTcxMjA0MDM0MjQ5WWhcNMjAxMjAzMDM0MjQ5WjBpMQswCQYDVQQLGwJ4\neDELMAkGA
1UECAwCeHgxGzAJBgNVBAAcManh4MQswCQYDVQQLDAJ4eDELMAkGA1UE
\nCwwCeHgxGzAJBgNVBAMMAnh4MRkwFwYJKoZIhvcNAQkBFgp4eEAXNjMuY29tMIIIB
\nlJlANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwZ5UJULajWr7p6FVwGRQRjFN\n2s8tZ/
6LC3X82fajpVsYqF1xqEuUDndDXVD09E4u83MS6HO6a3bIVQDp6/klnYld
\nniE6Vp8HH5BSKaCWKVg8IGWg1UM9wZFnlryi14KgmpIFmCu9nA8yV/6MZAe6RSDmb
\n3iyNBmiZ8aZhGw2pl1YwR+15MVqFFGB+7ExkziROI7L8CFCyCezK2/oOOvQsH1dz
\nQ8z1JXWdg8/9Zx7Ktvgwu5PQM3cjtSHX6iBPokMU8Z8TugLLtqQXKZOEgwajwvQ5\nnmf2DPkVgM08XAgALJ
cLigwD513koAdtJd5v+9irw+5LAuO3JclqwTwwy7u/YwwID\nAQABo1AwTjAdBgNVHQ4EFgQUo5A2tlU
+bcUfvGTD7wmEkhXKFjcwHwYDVR0jBBgw\nnFoAUo5A2tlU
+bcUfvGTD7wmEkhXKFjcwDAYDVR0TBAAUwAwEB/zANBgkqhkiG9w0B
\nAQsFAAOCAQEAwJ2rS6Mvqk3GfEpbocz2j3X7l1z8Sxoqg6ntwB+rezvK3mc9H0\nn83qcVeUcoH
+OA0IShyFN4FvRQL6X1hEheHarYwJK4agb231vb5erasuGO463eYEG\nnr4SfTuOm7SyiV2xxbaBKrXJtpBp4WLL/s
+LF+nklKjaOxmXUX0sM4CTA7uFJypY\nc8Tdr8IDDnQoUtMD8BrUCji+7lmMXRcC3Qi3oZJW76ja
+kZA5mKVFPd1ATih8TbA\nni34R7EQDtFeiSvBdeKRSPp8c0KT8H1B4IXNkkCQs2W5Xp4lm99+ZtLD4glw8x6lc
\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/
klnYldiE6Vp8HH5BSKaCWKVg8IGWg1\nUM9wZFnlryi14KgmpIFmCu9nA8yV/
6MZAe6RSDmb3iyNBmiZ8aZhGw2pl1YwR+15\nMVqFFGB+7ExkziROI7L8CFCyCezK2/
oOOvQsH1dzQ8z1JXWdg8/9Zx7Ktvgwu5PQ
\nM3cjtSHX6iBPokMU8Z8TugLLtqQXKZOEgwajwvQ5mf2DPkVgM08XAgALJcLigwD5\nn13koAdtJd5v+9irw
+5LAuO3JclqwTwwy7u/YwwIDAQABAoIBACU9S5fjD9/jTMA\nnDRs08A+gGgZUxLn0xk
+NAPX3LyB1tfdkCaFB8BccLzO6h3KZuwQOBPv6jkdvEDbx\nnNwyw3eA/
9GJslvKiHc0rejdvyPymaw9I8MA7NbXHaJrY7KpQDQyk6sx+aUTcy5jg\nniMXLWdwXYHhJ/
1HVOo603oZyiS6HZeYU089NDUCx+1Sji3e5Ke0gPVXEqCq1O11\n\nnrh24bMxmwZo4PKBWdcMBN5Zf/4ij9vrZE
+fFzW7vGBO48A5lvZxWU2U5t/OZQRtN
\n1uLOHmMFA0FIF2aWbTVfwdUWAFsvAOkHj9VVB8XOUwKOuUektdkfAlvrXmsFrO/H\n\nnyDeYYPkCgYEA/
S55CBbR0sMXP5Z56uRn8JHApZJhgkgvYr+FqDUq/e92nAzf01P\n\nRoEBUajwrnf1ycevN/
SDfbtWzq2XJGqhWdJmtpO16b7KBsC6BdRcH6dnOYh31jgA
\nnvABMIP3wzl4zSVTyxRE8LDuboytF1mSCeV5tHYPQTZNwrpLdnLQhywcCgYEAw8Yc\n\nnUk/eiFr3hfH/
ZohMfV5p82Qp7DNIGRzw8YTVG/3+vNXrAXW1VhugNhQY6L+zLtlC
\nhNk84ooup0m3YCg0hvlNqJuvzfuszQgtjTXyaE0cEwsjUusOmiuj09vVx/3U7siK
\nnaJd2ICPCvQ6Q8tdi8jV320gMs05AtaBkZdsiWUCgYEAtLw4Kk4f+xtKDFsrLUNf
\n75wcqhWVBiwBp7yQ7UX4EysJPKZcHMRTk0EEcAbpyaJZE3l44vjp5ReXIHNLmfPs
\nnuv134J4Rfot0LN3n7cFrAi2+wpNo+MOBwrNzpRmijGP2uKKRq4JiMjFbKV/6utGF
\nUp7VxfvS904JYpGgAZctiIECgYA1A6nZtF0riY6ry/uAdXpZHL8ONNqRZtWoT0kD
\n79otSVu5ISiRbaGcXsDExC52oKrSDAgFtbqQUiEOFG09UCXf0R6HwRkba2CiDwve
\nnyHQLQI5Qrdxz8Mk0glrNrSM4FamcW9vi9z4kCbQyoC5C+4gqeUURpDikQBWp2Y4\n\nn2ct/
bQKBgHv8qCsQTZphOxc31BJPa2xVhuv18cEU3XLURvFUZ/1f43JhLp7gynS2\n\nnep+
+LKUi9D0VGXY8bqvffjBECeCeu85vl8NpCXwe/LoVoln+7KaVIZMwqoGMfgNL\n\nnnEqm7HWkNxBHf8A6En/
Ijleudd5sf9e/x+TJN1Xhnt9W6pe7Fk1\n\n-----END RSA PRIVATE KEY-----",
  "certificate": "-----BEGIN CERTIFICATE-----
\nMIIDpTCCAo2gAwIBAgIJAKdmmOBYnFvoMA0GCSqGSIb3DQEBCwUAMGkxCzAJBgNV
\nBAYTAnh4MQswCQYDVQQLDAJ4eDELMAkGA1UEBwwCeHgxGzAJBgNVBAAoManh4MQsw
\nCQYDVQQLDAJ4eDELMAkGA1UEAwwCeHgxGTAXBgkqhkiG9w0BQCQEWCh4QDE2My5j
\nb20wHhcNMTcxMjA0MDM0MjQ5WWhcNMjAxMjAzMDM0MjQ5WjBpMQswCQYDVQQLGwJ4\neDELMAkGA
1UECAwCeHgxGzAJBgNVBAAcManh4MQswCQYDVQQLDAJ4eDELMAkGA1UE
\nCwwCeHgxGzAJBgNVBAMMAnh4MRkwFwYJKoZIhvcNAQkBFgp4eEAXNjMuY29tMIIIB
\nlJlANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwZ5UJULajWr7p6FVwGRQRjFN\n2s8tZ/
6LC3X82fajpVsYqF1xqEuUDndDXVD09E4u83MS6HO6a3bIVQDp6/klnYld
\nniE6Vp8HH5BSKaCWKVg8IGWg1UM9wZFnlryi14KgmpIFmCu9nA8yV/6MZAe6RSDmb
\n3iyNBmiZ8aZhGw2pl1YwR+15MVqFFGB+7ExkziROI7L8CFCyCezK2/oOOvQsH1dz
\nQ8z1JXWdg8/9Zx7Ktvgwu5PQM3cjtSHX6iBPokMU8Z8TugLLtqQXKZOEgwajwvQ5\nnmf2DPkVgM08XAgALJ
cLigwD513koAdtJd5v+9irw+5LAuO3JclqwTwwy7u/YwwID\nAQABo1AwTjAdBgNVHQ4EFgQUo5A2tlU
+bcUfvGTD7wmEkhXKFjcwHwYDVR0jBBgw\nnFoAUo5A2tlU
+bcUfvGTD7wmEkhXKFjcwDAYDVR0TBAAUwAwEB/zANBgkqhkiG9w0B
\nAQsFAAOCAQEAwJ2rS6Mvqk3GfEpbocz2j3X7l1z8Sxoqg6ntwB+rezvK3mc9H0\nn83qcVeUcoH
+OA0IShyFN4FvRQL6X1hEheHarYwJK4agb231vb5erasuGO463eYEG\nnr4SfTuOm7SyiV2xxbaBKrXJtpBp4WLL/s
+LF+nklKjaOxmXUX0sM4CTA7uFJypY\nc8Tdr8IDDnQoUtMD8BrUCji+7lmMXRcC3Qi3oZJW76ja
+kZA5mKVFPd1ATih8TbA\nni34R7EQDtFeiSvBdeKRSPp8c0KT8H1B4IXNkkCQs2W5Xp4lm99+ZtLD4glw8x6lc
\ni1YhgnQbn5E0hz55OLu5jvOkKQjPCW+8Kg==\n-----END CERTIFICATE-----",
  "type": "server"
}
```



```
6LC3X82fajpVsYqF1xqEuUDndDXVD09E4u83MS6HO6a3bIVQDp6/klnYld
\niE6Vp8HH5BSKaCWKVg8IGWg1UM9wZFnlryi14KgmpIFmcu9nA8yV/6MZAe6RSDmb
\n3iyNBmiZ8aZhGw2p11YwR+15MVqFFGB+7ExkziROi7L8CFCyCezK2/oOOvQsH1dz
\nQ8z1JXWdg8/9Zx7Ktvgwu5PQM3cJtSHX6iBPokMU8Z8TugLLTqQXKZOEgwajwvQ5\nnmf2DPkVgM08XAgalJ
cLigwD513koAdtjd5v+9irw+5LAuO3JclqwTvvy7u/YwwID\nnAQABo1AwTjAdBgNVHQ4EFgQUo5A2tlu
+bcUfvGTD7wmEkhXKFjcwHwYDVR0jBBgw\nnFoAUo5A2tlu
+bcUfvGTD7wmEkhXKFjcwDAYDVR0TBAAUwAwEB/zANBgkqhkiG9w0B
\nnAQsFAAOCAQEAJ2rS6Mvlqk3GfEpboezx2J3X7l1z8Sxoqg6ntwB+rezvK3mc9H0\nn83qcVeUcoH
+0A0lSHyFN4FvRQL6X1hEheHarYwJK4agb231vb5erasuGO463eYEG\nnr4SfTuOm7SviV2xxbaBKrXJtpBp4WLL/s
+LF+nklKjaOxkmxUX0sM4CTA7uFJypY\nnc8Tdr8IDDNqoUtMD8BrUCji+7lmMXRcC3Qi3oZJW76ja
+kZA5mKVFPd1ATih8TbA\nni34R7EQDtFeiSvBdeKRsPp8c0KT8H1B4lXNkkCQs2WX5p4lm99+ZtLD4glw8x6lc
\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.

AAppendix

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	The request body is null or empty. The 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	The API response is null or invalid.	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	The load balancer does not exist.	The load balancer does not exist.	Check the load balancer ID.

Status Code	Error Codes	Error Message	Description	Solution
400	ELB.1004	The query condition is invalid.	Invalid query condition.	Change the query condition.
400	ELB.1005	Invalid update request parameters.	Failed to modify the load balancer.	Check the parameters.
400	ELB.1007	Querying the internal load balancer failed.	Failed to query the details of the private network load balancer.	Contact customer service.
400	ELB.1008	This load balancer has members associated.	Failed to delete the load balancer.	Change the parameter settings.
400	ELB.1010	Querying the load balancer quota failed.	Failed to query the quota.	Contact customer service.
400	ELB.1011	Invalid private key or certificate content.	Invalid private or public key of the server certificate.	Enter a valid private or public key.
400	ELB.1012	Failed to create the relationship between resources and the user.	Failed to create the relationship between resources and the user.	Contact customer service.
400	ELB.1013	Quota modification failed. The quota set in the Cloud Eye alarm rule is excessively high.	The quota modification failed due to an excessively high quota setting in the Cloud Eye alarm rule.	Contact customer service.
400	ELB.1014	Failed to query the relationship between resources and the user.	Failed to query the relationship between resources and the user.	Contact customer service.

Status Code	Error Codes	Error Message	Description	Solution
400	ELB.1015	Updating the load balancer failed.	Failed to modify the load balancer.	Check the parameters.
400	ELB.1018	This load balancer has members associated.	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	Incorrect load balancer ID.	Incorrect load balancer ID.	Change the parameter settings.
400	ELB.1021	Invalid request parameters. Invalid load balancer name.	Invalid load balancer name.	Change the name.
400	ELB.1025	Invalid update request parameters. The load balancer name is too long.	The load balancer name exceeds the length limit.	Change the name.
400	ELB.1031	Invalid request parameters. The load balancer description is too long.	The load balancer description exceeds the length limit.	Change the description.
400	ELB.1035	Invalid update request parameters. Invalid load balancer name.	Invalid load balancer name.	Change the name.
400	ELB.1041	Invalid request parameters. Invalid load balancer type.	Invalid load balancer type.	Change the parameter settings.

Status Code	Error Codes	Error Message	Description	Solution
400	ELB.1045	Invalid update request parameters. The load balancer description is too long.	The load balancer description exceeds the length limit.	Change the description.
400	ELB.1051	Invalid request parameters. Invalid load balancer bandwidth.	Invalid bandwidth configured for the load balancer.	Modify the bandwidth.
400	ELB.1061	Invalid request parameters. Parameters vip_address and vip_subnet_id are null.	The EIP or subnet ID is left blank.	Enter a valid EIP or subnet ID.
400	ELB.1071	Invalid request parameters. vip_address is not valid.	Invalid EIP.	Enter a valid EIP.
400	ELB.1081	Invalid request parameters. vpc_id is empty.	The VPC ID is left blank.	Enter a valid VPC ID.
400	ELB.1101	The EIP already exists.	The EIP already exists.	Enter another EIP.
400	ELB.1110	The API version could not be found.	The API version does not exist.	Contact customer service.
400	ELB.1201	Obtaining the token failed.	Failed to obtain the token.	Contact customer service.
400	ELB.1202	enterprise_project_id cannot be empty.	Verification of the enterprise project ID failed.	Check the enterprise project ID.

Status Code	Error Codes	Error Message	Description	Solution
400	ELB.1204	Binding failed.	Failed to associate the load balancer with the enterprise project.	Contact customer service.
400	ELB.2002	Invalid request parameters for removing the backend server.	Failed to remove the backend server because the parameters are invalid.	Change the parameter settings.
400	ELB.2003	Querying the member failed.	Failed to query the backend server.	Contact customer service.
400	ELB.2005	Updating the member failed.	Failed to update the backend server.	Contact customer service.
400	ELB.2010	Invalid listener ID length.	The listener ID exceeds the length limit.	Change the listener ID.
400	ELB.2011	The listener does not exist.	The listener does not exist.	Ensure that the listener exists.
400	ELB.2012	The member does not exist.	The backend server does not exist.	Ensure that the backend server exists.
400	ELB.2020	Invalid listener ID.	Invalid listener ID.	Change the listener ID.
400	ELB.2021	Invalid request parameters. The member IP address is null.	Invalid backend server IP address.	Check the backend server IP address.
400	ELB.3001	Creating the EIP failed.	Failed to assign the EIP.	Contact customer service.

Status Code	Error Codes	Error Message	Description	Solution
400	ELB.3002	Deleting the EIP failed.	Failed to release the EIP.	Contact customer service.
400	ELB.3003	Querying the EIP failed.	Failed to query the EIP.	Contact customer service.
400	ELB.3004	Querying EIPs failed.	Failed to query EIPs.	Contact customer service.
400	ELB.4001	Creating the EIP failed.	Failed to assign the EIP.	Contact customer service.
400	ELB.4002	Deleting the EIP failed.	Failed to release the EIP.	Contact customer service.
400	ELB.4003	Querying the EIP failed.	Failed to query the EIP.	Contact customer service.
400	ELB.4004	Querying EIPs failed.	Failed to query EIPs.	Contact customer service.
400	ELB.4005	Updating the EIP 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	Querying the 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	Updating the bandwidth failed.	Failed to modify the bandwidth.	Contact customer service.
400	ELB.5013	Invalid private key or certificate content.	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 long.	The certificate ID is not a 32-character string.	Enter a valid certificate ID.

Status Code	Error Codes	Error Message	Description	Solution
400	ELB.5033	Failed to update the certificate.	Failed to modify the certificate.	Contact customer service.
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 used 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	Invalid listener ID.	Invalid listener ID.	Change the listener ID.
400	ELB.6011	Invalid request parameters. The listener name is too long.	The listener name exceeds the length limit.	Change the name.
400	ELB.6015	The listener property cannot be updated.	The listener property cannot be modified.	Select a property that can be modified.

Status Code	Error Codes	Error Message	Description	Solution
400	ELB.6021	Invalid request parameters. Invalid listener name.	Invalid listener name.	Change the name.
400	ELB.6025	Invalid update request parameters. The listener name is too long.	The listener name exceeds the length limit.	Change the name.
400	ELB.6030	The listener has not been associated with any load balancer.	The listener does not belong to any load balancer.	Check the listener ID.
400	ELB.6031	Invalid request parameters. The listener description is too long.	The listener description exceeds the length limit.	Change the description.
400	ELB.6035	Invalid update request parameters. Invalid listener name.	Invalid listener name.	Change the name.
400	ELB.6040	The load balancer that the listener is associated with does not exist.	The load balancer that the listener is associated with does not exist.	Check the load balancer ID.
400	ELB.6041	Invalid request parameters. The listener port must be within the range of 1 to 65535.	Invalid port number.	Change the port number.

Status Code	Error Codes	Error Message	Description	Solution
400	ELB.6045	Invalid update request parameters. The listener description is too long.	The listener description exceeds the length limit.	Change the description.
400	ELB.6051	Invalid request parameters. Invalid load balancing algorithm.	Invalid load balancing algorithm.	Change the load balancing algorithm.
400	ELB.6061	Invalid request parameters. Invalid listener protocol.	Invalid listener protocol.	Change the protocol.
400	ELB.6071	Invalid request parameters. Invalid backend protocol.	Invalid backend protocol.	Change the protocol.
400	ELB.6200	Load balancer *** already has a listener with protocol_port of ***.	The port number is in use.	Change the port number.
400	ELB.7000	The listener ID must not be null.	The listener ID is left blank.	Change the listener ID.
400	ELB.7001	Invalid health check interval.	Invalid update condition.	Change the update condition.
400	ELB.7002	Invalid health check deletion condition.	Invalid deletion condition.	Change the deletion condition.
400	ELB.7004	Invalid health check query condition.	Invalid query condition.	Change the query condition.

Status Code	Error Codes	Error Message	Description	Solution
400	ELB.7010	The health check listener does not exist.	The listener with which the health check is associated does not exist.	Change the listener ID.
400	ELB.7014	The health check does not exist.	The health check does not exist.	Check the health check ID.
400	ELB.7020	The health check does not exist.	The health check does not exist.	Change the health check ID.
400	ELB.8001	Creating the security group failed.	Failed to create the security group.	Contact customer service.
400	ELB.8101	Creating the VPC failed.	Failed to create the VPC.	Contact customer service.
400	ELB.8102	Deleting the VPC failed.	Failed to delete the VPC.	Contact customer service.
400	ELB.8103	Querying the VPC failed.	Failed to query the VPC.	Contact customer service.
400	ELB.8201	Creating the subnet failed.	Failed to create the subnet.	Contact customer service.
400	ELB.8202	Deleting the subnet failed.	Failed to delete the subnet.	Contact customer service.
400	ELB.8203	Querying the subnet failed.	Failed to query the subnet.	Contact customer service.
400	ELB.8902	Invalid input for '%s'.	Invalid input parameters.	Check input parameters.

Status Code	Error Codes	Error Message	Description	Solution
400	ELB.8909	Certificates with multiple domains are not supported by dedicated load balancers.	Certificates with multiple domains are not supported by dedicated load balancers.	Check input parameters.
400	ELB.8934	The number of available IP addresses in the subnet on the downstream plane is insufficient.	The number of available IP addresses in the subnet on the downstream plane is insufficient.	Check your request based on the error message.
400	ELB.8938	The IP member is supported only when the pool protocol is %s.	Invalid input parameters.	Add members to supported pools or pass parameter subnet_cidr_id.
400	ELB.8939	The load balancer's ip_target_enable must be true when adding IP members.	Invalid input parameters.	Set ip_target_enable to false or pass parameter subnet_cidr_id.
400	ELB.8950	Resources cannot be allocated to the load balancer.	Resources cannot be allocated to the load balancer.	Contact customer service.
400	ELB.8959	The %s flavor field does not support update from %s to %s.	Invalid input parameters when updating the flavor.	Check input parameters.
400	ELB.9001	Creating the VM failed.	Failed to create the VM.	Contact customer service.
400	ELB.9002	Deleting the VM failed.	Failed to delete the VM.	Contact customer service.

Status Code	Error Codes	Error Message	Description	Solution
400	ELB.9003	Querying the VM failed.	Failed to query details of the VM.	Contact customer service.
400	ELB.9006	Updating the VM port failed.	Failed to update the port bound to the VM.	Contact customer service.
400	ELB.9007	Binding the VM port failed.	Failed to bind the port to the VM.	Contact customer service.
400	ELB.9023	Querying the image failed.	Failed to query the image.	Contact customer service.
400	ELB.9033	Querying the VM flavor failed.	Failed to query the VM specifications.	Contact customer service.
400	ELB.9043	Querying the VM port failed.	Failed to query the port bound to the VM.	Contact customer service.
400	ELB.9061	Querying the SMN topic failed.	Failed to query the SMN topic.	Contact customer service.
400	ELB.9062	Creating the SMN topic failed.	Failed to create the SMN topic.	Contact customer service.
400	ELB.9063	Querying the SMN subscription failed.	Failed to query the SMN subscription.	Contact customer service.
400	ELB.9064	Creating the SMN subscription failed.	Failed to create the SMN subscription.	Contact customer service.
400	ELB.9800	The 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	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	Listener protocol in the request body 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	Not enough resource quotas.	Contact customer to expand quotas.
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	The number of load balancers exceeds the 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	Invalid token. Authentication required.	The token is empty.	Enter a valid token that has not expired.

Status Code	Error Codes	Error Message	Description	Solution
403	ELB.2001	Creating the member failed. The total number of members exceeds the upper limit.	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	The number of listeners reaches the limit.	The number of listeners reaches the limit.	Request a higher quota or delete listeners that are no longer needed.
403	ELB.8962	The feature is not supported.	The feature is not supported.	Contact customer service.
403	ELB.9802	elb:logtanks:create is not obtained.	Authentication failed.	Ensure that you have the permission to perform this operation.
403	ELB.9803	elb:loadbalancers:list is not obtained.	Authentication failed.	Ensure that you have the permission to perform this operation.
403	ELB.9804	elb:loadbalancers:list is not obtained.	Authentication failed.	Ensure that you have the permission to perform this operation.
404	ELB.1002	The load balancer is not found.	The load balancer does not exist.	Change the load balancer ID.
404	ELB.8904	%s %s could not be found.	The resource could not be found.	Please check the parameters.
409	ELB.8905	Quota exceeded for resources: %s	Not enough resource quotas.	Contact customer service.

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 server error.	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/a4adasfjljaaakla12334jklga9sasfg"
      },
      "id": "a4adasfjljaaakla12334jklga9sasfg",
      "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

