

Elastic Load Balance User Guide

User Guide

Issue 01
Date 2025-02-19



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 User Guide for Dedicated Load Balancers.....	1
1.1 Using a Dedicated Load Balancer.....	1
1.2 Permissions Management.....	5
1.2.1 Creating a User and Granting Permissions.....	5
1.2.2 Creating a Custom Policy.....	6
1.3 Load Balancer.....	8
1.3.1 Dedicated Load Balancer Overview.....	8
1.3.2 Creating a Dedicated Load Balancer.....	12
1.3.3 Enabling or Disabling Modification Protection for Dedicated Load Balancers.....	21
1.3.4 Modifying the Basic Configurations of a Dedicated Load Balancer.....	22
1.3.5 Modifying the Network Configurations of a Dedicated Load Balancer.....	24
1.3.6 Exporting Dedicated Load Balancers.....	27
1.3.7 Deleting a Dedicated Load Balancer.....	28
1.3.8 Copying a Dedicated Load Balancer.....	29
1.3.9 Enabling or Disabling a Load Balancer.....	31
1.4 Listener.....	32
1.4.1 Listener Overview.....	32
1.4.2 Network Listeners.....	37
1.4.2.1 Adding a TCP Listener.....	37
1.4.2.2 Adding a UDP Listener.....	39
1.4.2.3 Adding a UDP Listener (with a QUIC Backend Server Group Associated).....	42
1.4.2.4 Adding a TLS Listener.....	43
1.4.3 Application Listeners.....	47
1.4.3.1 Adding an HTTP Listener.....	47
1.4.3.2 Adding an HTTPS Listener.....	51
1.4.3.3 Adding a QUIC Listener.....	57
1.4.3.4 Forwarding Policy.....	61
1.4.3.5 Advanced Forwarding.....	65
1.4.3.5.1 Advanced Forwarding.....	65
1.4.3.5.2 Managing an Advanced Forwarding Policy.....	76
1.4.3.6 HTTP Headers.....	78
1.4.3.7 HTTP/2.....	80
1.4.4 Modifying a Listener.....	82

1.5 Backend Server Group.....	84
1.5.1 Backend Server Group Overview.....	84
1.5.2 Creating a Backend Server Group.....	88
1.5.3 Controlling Traffic Distribution.....	96
1.5.3.1 Load Balancing Algorithms.....	96
1.5.3.2 Sticky Session.....	101
1.5.3.3 Slow Start.....	104
1.5.4 Changing a Backend Server Group.....	105
1.5.5 Managing a Backend Server Group.....	106
1.6 Backend Server.....	107
1.6.1 Backend Server Overview.....	107
1.6.2 Security Group and Network ACL Rules.....	109
1.6.3 Adding Backend Servers in the Same VPC as a Load Balancer.....	112
1.6.4 Adding Backend Servers in a Different VPC from a Load Balancer.....	114
1.7 Health Check.....	118
1.7.1 Health Check.....	118
1.7.2 Configuring a Health Check.....	126
1.8 Security.....	130
1.8.1 Transfer Client IP Address.....	130
1.8.2 TLS Security Policy.....	131
1.8.3 SNI Certificate.....	142
1.8.4 Certificate.....	144
1.8.4.1 Certificate Overview.....	144
1.8.4.2 Adding a Certificate.....	147
1.8.4.3 Managing Certificates.....	150
1.8.4.4 Binding or Replacing a Certificate.....	151
1.8.4.5 Replacing the Certificate Bound to Different Listeners.....	152
1.8.5 Access Control.....	152
1.8.5.1 What Is Access Control?.....	152
1.8.5.2 IP Address Group.....	154
1.8.6 Protection for Mission-Critical Operations.....	157
1.9 Access Logging.....	160
1.10 Tags and Quotas.....	172
1.10.1 Tag.....	172
1.10.2 Quotas.....	174
1.11 Cloud Eye Monitoring.....	175
1.11.1 Monitoring ELB Resources.....	176
1.11.2 ELB Monitoring Metrics.....	177
1.11.3 Event Monitoring.....	216
1.11.4 Viewing Traffic Usage.....	217
1.12 Auditing.....	219
1.12.1 Key Operations Recorded by CTS.....	220

1.12.2 Viewing Traces.....	221
2 User Guide for Shared Load Balancers.....	224
2.1 Permissions Management.....	224
2.1.1 Creating a User and Granting Permissions.....	224
2.1.2 Creating a Custom Policy.....	225
2.2 Load Balancer.....	227
2.2.1 Shared Load Balancer Overview.....	227
2.2.2 Creating a Shared Load Balancer.....	229
2.2.3 Configuring Modification Protection for Shared Load Balancers.....	233
2.2.4 Changing the Network Configurations of a Shared Load Balancer.....	234
2.2.5 Deleting a Shared Load Balancer.....	235
2.2.6 Enabling or Disabling a Shared Load Balancer.....	235
2.2.7 Enabling Guaranteed Performance for a Shared Load Balancer.....	236
2.3 Listener.....	237
2.3.1 Listener Overview.....	237
2.3.2 Adding a TCP Listener.....	239
2.3.3 Adding a UDP Listener.....	241
2.3.4 Adding an HTTP Listener.....	242
2.3.5 Adding an HTTPS Listener.....	245
2.3.6 Forwarding Policy.....	248
2.3.7 HTTP/2.....	254
2.3.8 Modifying a Listener.....	256
2.3.9 Deleting a Listener.....	257
2.4 Backend Server Group.....	258
2.4.1 Backend Server Group Overview.....	258
2.4.2 Creating a Backend Server Group.....	259
2.4.3 Controlling Traffic Distribution.....	263
2.4.3.1 Load Balancing Algorithms.....	264
2.4.3.2 Sticky Session.....	268
2.4.4 Changing a Backend Server Group.....	271
2.4.5 Managing a Backend Server Group.....	272
2.5 Backend Server.....	273
2.5.1 Backend Server Overview.....	273
2.5.2 Security Group and Network ACL Rules.....	274
2.5.3 Cloud Servers.....	277
2.6 Health Check.....	278
2.6.1 Health Check.....	278
2.6.2 Enabling or Disabling Health Check.....	283
2.7 Security.....	285
2.7.1 Transfer Client IP Address.....	286
2.7.2 SNI Certificate.....	287
2.7.3 TLS Security Policy.....	288

2.7.4 Access Control.....	294
2.7.4.1 What Is Access Control?.....	294
2.7.4.2 IP Address Group.....	295
2.7.5 Certificate.....	299
2.7.5.1 Certificate Overview.....	299
2.7.5.2 Adding a Certificate.....	302
2.7.5.3 Managing Certificates.....	305
2.7.5.4 Binding or Replacing a Certificate.....	306
2.7.5.5 Replacing the Certificate Bound to Different Listeners.....	306
2.7.6 Protection for Mission-Critical Operations.....	307
2.8 Access Logging.....	310
2.9 Tags and Quotas.....	321
2.9.1 Tag.....	321
2.9.2 Quotas.....	323
2.10 Cloud Eye Monitoring.....	324
2.10.1 Monitoring ELB Resources.....	325
2.10.2 Monitoring Metrics.....	326
2.10.3 Viewing Traffic Usage.....	345
2.11 Auditing.....	347
2.11.1 Key Operations Recorded by CTS.....	347
2.11.2 Viewing Traces.....	348
3 Self-service Troubleshooting.....	351
3.1 Overview.....	351
3.2 Troubleshooting an Unhealthy Backend Server.....	351
3.3 Other Issues.....	355
4 Appendix.....	357
4.1 Configuring the TOA Module.....	357

1 User Guide for Dedicated Load Balancers

1.1 Using a Dedicated Load Balancer

If you are using a dedicated load balancer for the first time, you can start from this section.

ELB automatically distributes incoming traffic across multiple backend servers based on the routing policies you configure. It expands the service capabilities of your applications and improves their availability by eliminating single points of failure (SPOFs).

ELB Architecture

Figure 1-1 ELB architecture

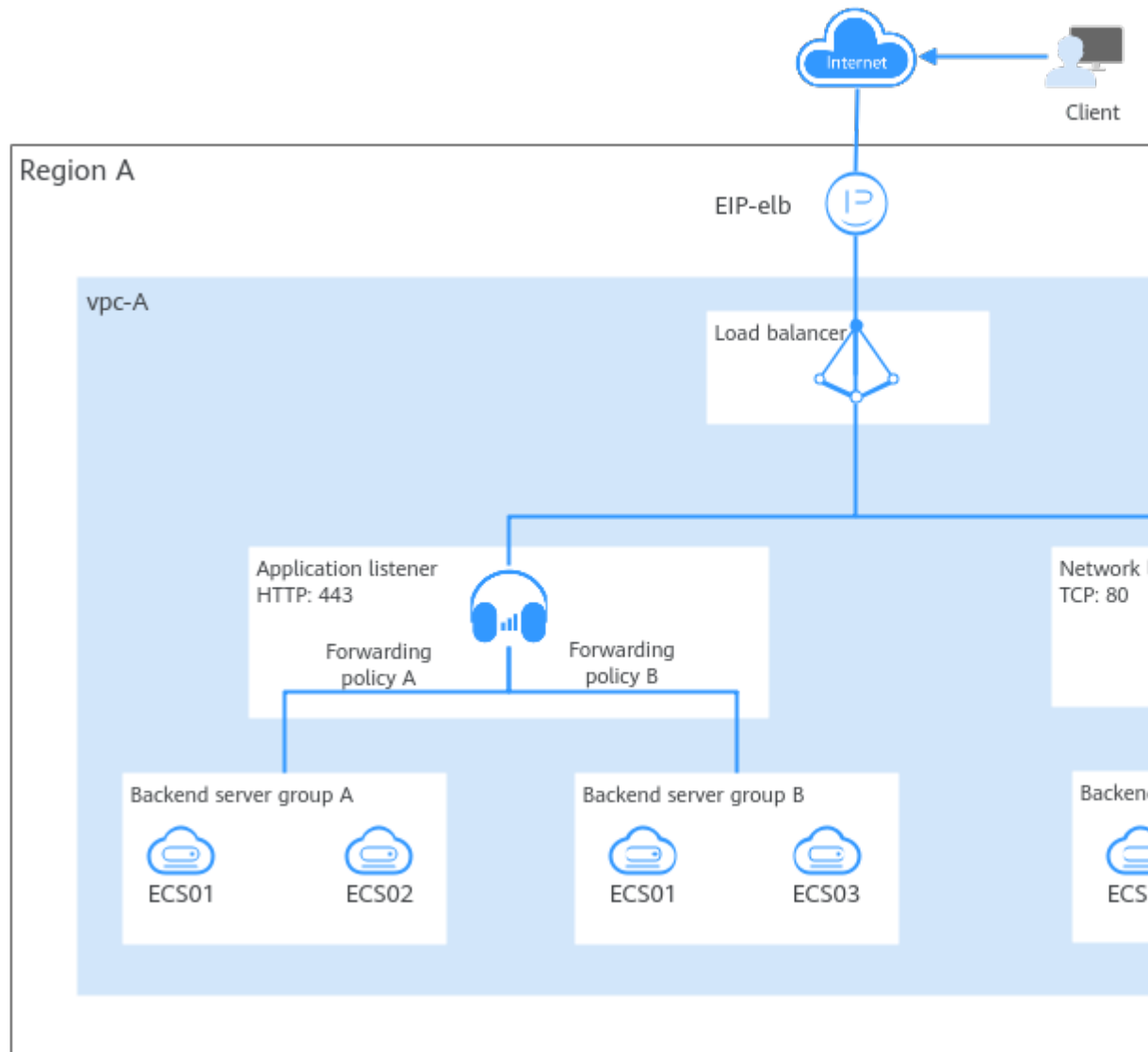


Table 1-1 ELB components

Component	Description	Reference
Load balancer	Distributes incoming traffic across backend servers in one or more AZs. Before using a load balancer, you need to add at least one listener to it.	Dedicated Load Balancer Overview

Component	Description	Reference
Listener	<p>Works as the minimum service unit. It uses a protocol and port (for example, TCP port 80) you have specified to check requests from clients and route the requests to associated backend servers.</p> <p>Each load balancer must have at least one listener to check and distribute traffic. You can add different types of listeners to distribute traffic using different protocols and ports.</p> <p>Network listeners forward traffic to the default backend server group, while application listeners forward traffic based on the forwarding policies you configure.</p>	Listener Overview
Forwarding policy	<p>Determines how application load balancers distribute traffic across one or more backend server groups. Forwarding policies can be only configured for application listeners.</p> <p>Application load balancers distribute Layer 7 requests more efficiently. They support various protocols and forwarding policies to suit your service needs.</p>	Advanced Forwarding
Backend server group	<p>Contains one or more backend servers to process requests distributed by load balancers.</p> <p>A backend server group can be created independently. A backend server group can be associated with one or more load balancers.</p>	Backend Server Group Overview
Backend server	<p>Processes client requests. A backend server can be an ECS, BMS, supplementary network interface, or IP address. If a supplementary network interface or an IP address is added as a backend server, the server with the supplementary network interface attached or using the IP address processes client requests.</p> <p>ELB periodically sends requests to backend servers to check whether they can process requests. This process is called health check. If a backend server is identified as unhealthy, the load balancer will stop routing requests to it.</p>	Backend Server Overview

Procedure for Using a Dedicated Load Balancer

The following describes how to quickly create and use a dedicated load balancer.

Figure 1-2 Procedure for using a dedicated load balancer



Procedure	What to Do
Creating a Dedicated Load Balancer	<p>Create a dedicated load balancer and be careful with the following configurations:</p> <ul style="list-style-type: none"> • Basic information: type, billing mode, region, and AZ. • Specifications: elastic or fixed specifications; network or application load balancing, or both. • Network configuration: network type (private IPv4 or IPv6), VPC, and subnet planning.
Creating a Backend Server Group	<p>Create a backend server group and add backend servers to the group for easier management and scheduling.</p> <p>You can create a backend server group first and select it when creating a dedicated load balancer. Plan the backend protocol appropriately because the backend protocol of each backend server group must match the frontend protocol of the associated listeners.</p>
<ul style="list-style-type: none"> • Network Listeners • Application Listeners 	<p>Add listeners and choose the protocols and ports based on service requirements.</p> <ul style="list-style-type: none"> • Application listeners (HTTP/HTTPS/QUIC): work well for workloads that require high performance at Layer 7, such as real-time audio and video, interactive livestreaming, and game applications. • Networking listeners (TCP/UDP/TLS): are good for heavy-traffic and high-concurrency workloads at Layer 4, such as file transfer, instant messaging, and online video applications.
Advanced Forwarding	<p>Configure advanced forwarding policies for application listeners to forward traffic to specified backend server groups based on the domain name, path, HTTP request method, HTTP header, query string, and CIDR block.</p>

Backend Server Group and Listener Protocols

You can associate a backend server group with different listeners or different dedicated load balancers under the same enterprise project.

The backend protocol of each backend server group must match the frontend protocol of the associated listeners as described in [Table 1-2](#).

Table 1-2 The frontend and backend protocol

Load Balancer Specification	Frontend Protocol	Backend Protocol
Network load balancing	TCP	TCP

Load Balancer Specification	Frontend Protocol	Backend Protocol
Network load balancing	UDP	<ul style="list-style-type: none">• UDP• QUIC
Network load balancing	TLS	<ul style="list-style-type: none">• TLS• TCP
Application load balancing	HTTP	HTTP
Application load balancing	HTTPS	<ul style="list-style-type: none">• HTTP• HTTPS• gRPC
Application load balancing	QUIC	<ul style="list-style-type: none">• HTTP• HTTPS• gRPC

 NOTE

TLS, gRPC, and QUIC will be available in more regions. You can see which regions support them on the console.

1.2 Permissions Management

1.2.1 Creating a User and Granting Permissions

Use [IAM](#) to implement fine-grained permissions control over your ELB resources. With IAM, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing ELB resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust another Huawei Cloud account or cloud service to perform efficient O&M on your ELB resources.

Skip this section if your Huawei Cloud account does not need individual IAM users.

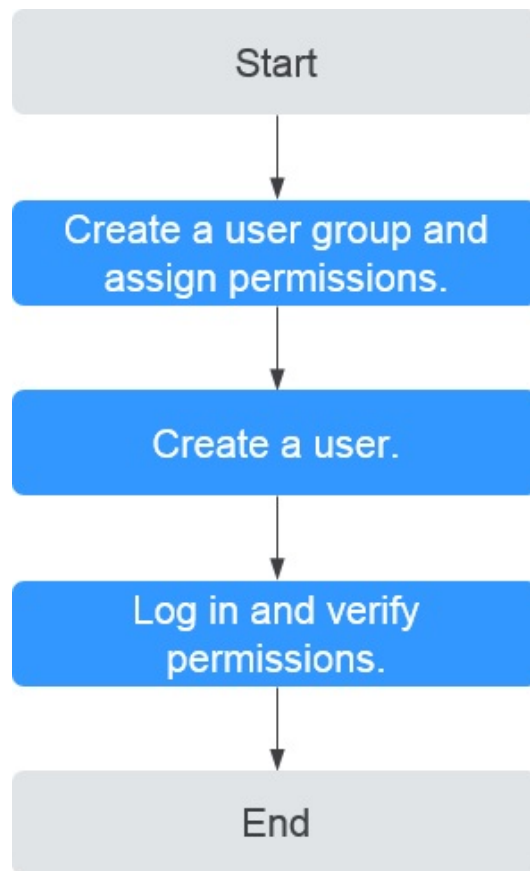
This following describes the procedure for granting permissions.

Prerequisites

You have learned about ELB policies and can select the appropriate policies based on service requirements. Learn about [permissions](#) supported by ELB. For the permissions of other services, see [System Permissions](#).

Process Flow

Figure 1-3 Process for granting ELB permissions



1. **Create a user group and assign permissions.**
Create a user group on the IAM console, and assign the **ELB ReadOnlyAccess** policy to the group.
2. **Create a user and add it to a user group.**
Create a user on the IAM console and add the user to the group created in 1.
3. **Log in** and verify permissions.
Log in to the ELB console by using the created user, and verify that the user only has read permissions for ELB.
 - Choose **Service List > Elastic Load Balance**. Then click **Buy Elastic Load Balancer** on the ELB console. If you cannot create a load balancer, the **ELB ReadOnlyAccess** policy has taken effect.
 - Choose any other service in **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the **ELB ReadOnlyAccess** policy has already taken effect.

1.2.2 Creating a Custom Policy

Custom policies can be created as a supplement to the system policies of ELB. For the actions supported for custom policies, see "Permissions Policies and Supported Actions" in the [Elastic Load Balance API Reference](#).

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Create a JSON policy or edit an existing one.

For details, see [Creating a Custom Policy](#). The following section contains examples of common ELB custom policies.

Example Custom Policies

- Example 1: Allowing users to update a load balancer

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "elb:loadbalancers:put"
      ]
    }
  ]
}
```

- Example 2: Denying load balancer deletion

A deny policy must be used in conjunction with other policies to take effect. If the permissions assigned to a user contain both Allow and Deny actions, the Deny actions take precedence over the Allow actions.

If you grant the system policy **ELB FullAccess** to a user but do not want the user to have the permission to delete load balancers defined in the policy, you can create a custom policy that rejects the deletion of load balancers and grant the **ELB FullAccess** and deny policies to the user, so that the user can perform all operations on ELB except deleting load balancers. The following is an example deny policy:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "elb:loadbalancers:delete"
      ]
    }
  ]
}
```

- Example 3: Defining permissions for multiple services in a policy

A custom policy can contain the actions of multiple services that are of the global or project-level type. The following is an example policy containing actions of multiple services:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "elb:loadbalancers:get",
        "elb:loadbalancers:list",
        "elb:loadbalancers:delete",
        "ecs:cloudServers:delete"
      ]
    }
  ]
}
```

```
}  
  ]  
}
```

1.3 Load Balancer

1.3.1 Dedicated Load Balancer Overview

A load balancer distributes incoming traffic across multiple backend servers. Before using a load balancer, you need to add at least one listener to it and associate one backend server with it.

Region

- You can choose the region nearest to your service deployment location to minimize network latency and speed up downloads.
- You can add servers in a different VPC from where the load balancer is created, or in an on-premises data center, by using private IP addresses of the servers. For details, see [Adding Backend Servers in a Different VPC from a Load Balancer](#).
- You can [connect VPCs in different regions](#).

AZ

Dedicated load balancers can be deployed across AZs. If you select multiple AZs, a load balancer is created in each selected AZ.

To reduce network latency and improve access speed, you are suggested to deploy your load balancer in the AZ where backend servers are running.

Load balancers in different AZs work in active-active or multi-active mode, and requests are distributed by the nearest load balancer in the same AZ.

Table 1-3 Disaster recovery planning

DR Solution	Application Scenario	Advantage
Select multiple AZs for a load balancer.	If the number of requests does not exceed what the largest specifications can handle, you can create a load balancer and select multiple AZs.	If the load balancer in an AZ goes down, the load balancer in other AZs takes over to route traffic.
Create multiple load balancers and select multiple AZs for each load balancer.	If the number of requests exceeds what the largest specifications can handle, you can create multiple load balancers and select multiple AZs for each load balancer.	If a load balancer in an AZ goes down, another load balancer in the same AZ or other AZs takes over to distribute traffic.

Table 1-4 Traffic distribution

Source	Traffic Distribution
Internet	If requests are from the Internet, the load balancer in each AZ you select routes the requests based on source IP addresses. If you select two AZs for a load balancer, the requests the load balancers can handle will be doubled.
Private network	<ul style="list-style-type: none">• If clients are in the same AZ as the load balancer, requests are distributed by the load balancer in this AZ. If the load balancer goes down, requests are distributed by the load balancer in another AZ. If the load balancer is healthy but the connections that the load balancer needs to handle exceed the amount defined in the specifications, service may be interrupted. To address this issue, you need to upgrade specifications. You can monitor traffic usage on private networks by AZ. <ul style="list-style-type: none">• If clients are in an AZ that is different from the load balancer, requests are distributed by the load balancer in each AZ you select based on source IP addresses.
Direct Connect connection	If requests are from a Direct Connect connection, the load balancer in the same AZ as the Direct Connect connection routes the requests. If the load balancer in this AZ goes down, requests are distributed by the load balancer in another AZ.
A VPC that is different from where the load balancer works	If requests are in a VPC that is different from where the load balancer works, the load balancer in the AZ where the original VPC subnet works routes the requests. If the load balancer in this AZ goes down, requests are distributed by the load balancer in another AZ.

Specifications

Dedicated load balancers provide a wide range of specifications to meet your requirements.

Network load balancers can route TCP, TLS, or UDP requests, while application load balancers route HTTP, QUIC, or HTTPS requests.

Select appropriate specifications based on your traffic volume and service requirements. For details, see [Specifications of Dedicated Load Balancers](#).

You can view the monitoring metrics on the Cloud Eye console to analyze the peak traffic and usage trends to select the specifications as needed.

For details, see [Table 1-5](#).

Table 1-5 Guide for selecting a specification

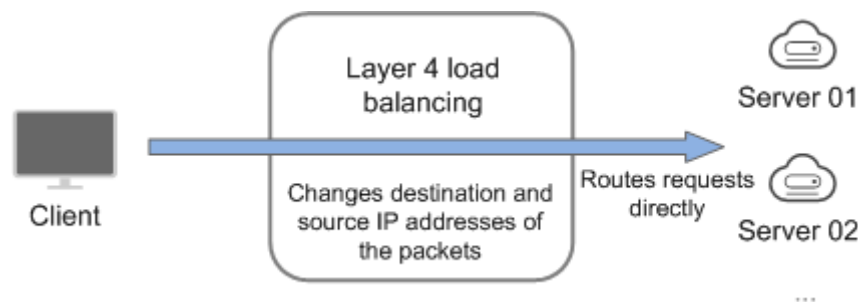
Specifications	Description
Network load balancing (TCP/UDP)	Pay attention to the maximum number of concurrent connections and consider maximum concurrent connections as a key metric. Estimate the maximum number of concurrent connections that a load balancer needs to handle and select the corresponding specification.
Application load balancing (HTTP/HTTPS)	Consider QPS as a key metric, which determines the service throughput of an application system. Estimate the QPS that a load balancer needs to handle and select the corresponding specification.

Protocols

ELB provides load balancing at both Layer 4 and Layer 7. Choose an appropriate protocol when you add a listener to a load balancer.

- Network load balancers work well for heavy-traffic workloads that need to handle massively concurrent requests at Layer 4, such as file transfer, instant messaging, and online video services.

Figure 1-4 Layer 4 load balancing



- Application load balancers handle Layer 7 requests and support advanced forwarding policies.

Figure 1-5 Layer 7 load balancing

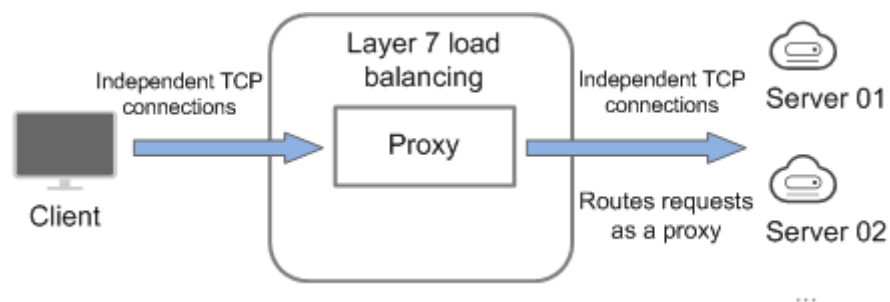


Table 1-6 Protocols

Protocol	Description
TCP/UDP	After receiving a request, the listener routes it directly to backend servers. In this process, the destination IP address in a packet is changed to the IP address of the backend server, and the source IP address to the private IP address of the load balancer. A connection is established after a three-way handshake between the client and the backend server, and the load balancer only forwards the data.
HTTP/HTTPS	Once the load balancer receives a request, it works as a proxy for backend servers and initiates a connection (three-way handshake) with the client. It then determines which backend server to route the request to based on the fields in the HTTP/HTTPS request header and the load balancing algorithm you select when you add the listener.

NOTE

ELB establishes persistent connections between the clients and the load balancers to reduce the costs of a large number of short connections. After a persistent connection is established, the client can keep sending HTTP or HTTPS requests to the load balancer until the connection times out.

Network Type

Dedicated load balancers can work on both public and private network.

Table 1-7 ELB network types

Network Type	Note	Application Scenarios
Load balancing on a public network	You need to assign an EIP or bind an existing EIP to this type of load balancers. They can receive requests from the Internet and route the requests to backend servers.	<ul style="list-style-type: none">• A load balancer is used as a single point of contact for clients when a group of servers provide services over the Internet.• Fault tolerance and fault recovery are necessary.

Network Type	Note	Application Scenarios
Load balancing on a private network	This type of load balancers has only private IP addresses and can be only accessed within a VPC. They receive requests from clients in a VPC and route the requests across backend servers in the same VPC.	<ul style="list-style-type: none">• There are multiple backend servers, and requests need to be evenly distributed across these servers.• Fault tolerance and fault recovery are necessary.• You do not want IP addresses of your physical devices to be exposed.

Backend Server

Before you use ELB, you need to create cloud servers, deploy required applications on them, and add the cloud servers to one or more backend server groups. When you create cloud servers, note the following:

- Cloud servers should be in the same region as the load balancer.
- Cloud servers that run the same OS are recommended so that you can manage them more easily.
- ELB does not support File Transfer Protocol (FTP), but supports Secure File Transfer Protocol (SFTP) on backend servers.

1.3.2 Creating a Dedicated Load Balancer

Scenarios

You have prepared everything required for creating a dedicated load balancer. For details, see [Dedicated Load Balancer Overview](#).

Notes and Constraints

- After a dedicated load balancer is created, its VPC cannot be changed. If you want to change the VPC, create another load balancer and select a different VPC.
- To ping the IP address of a dedicated load balancer, you need to add a listener to it.

Procedure

1. Go to the [Buy Elastic Load Balancer](#) page.
2. On the load balancer list page, click **Buy Elastic Load Balancer**.
Complete the basic configurations based on [Table 1-8](#).

Table 1-8 Parameters for configuring the basic information

Parameter	Description
Type	<p>Specifies the type of the load balancer. The type cannot be changed after the load balancer is created.</p> <p>Dedicated load balancers work well for heavy-traffic and high-concurrency workloads, such as large websites, cloud native applications, IoT, and multi-AZ disaster recovery applications.</p> <p>For details about the differences, see Differences Between Dedicated and Shared Load Balancers.</p>
Billing Mode	<p>Specifies the billing mode of the dedicated load balancer. You are charged for how long you use each load balancer.</p> <p>Pay-per-use: postpaid billing mode. You pay as you go and just pay for what you use. The load balancer usage is calculated by the second but billed every hour.</p>
Region	<p>Specifies the desired region. Resources in different regions cannot communicate with each other over internal networks. For lower network latency and faster access to resources, select the nearest region.</p>

Parameter	Description
AZ	<p>Specifies the AZ where the dedicated load balancer works. An AZ is a part of a region and has its own independent power supplies and networks. AZs are physically isolated but interconnected through internal networks.</p> <p>You can select multiple AZs for a load balancer to ensure high availability. If the load balancer in an AZ goes down, the load balancer in another AZ routes requests to backend servers to ensure service continuity and improve application reliability. For details about AZ planning, see AZ.</p> <p>If you select multiple AZs for a load balancer, its performance, such as the number of new connections and the number of concurrent connections, will multiply by the number of AZs. For example, a dedicated load balancer in an AZ can handle 20 million concurrent connections. If you select two AZs for a dedicated load balancer, it can handle up to 40 million concurrent connections.</p> <p>To reduce network latency and improve access speed, you are recommended to deploy your load balancer in the AZ where backend servers are running.</p> <p>NOTE</p> <ul style="list-style-type: none">• If you change the AZs of a load balancer, the load balancer may fail to route requests for several seconds. Plan the AZs in advance.• You are advised to change the AZs during off-peak hours. For details, see Changing an AZ.
Name	<p>Specifies the load balancer name. The name can contain:</p> <ul style="list-style-type: none">• 1 to 64 characters.• Letters, digits, underscores (_), hyphens (-), and periods (.).
Enterprise Project	<p>Specifies an enterprise project by which cloud resources and members are centrally managed.</p> <p>For details about creating and managing enterprise projects, see the Enterprise Management User Guide.</p>

3. Select specifications for the dedicated load balancer based on [Table 1-9](#).

Table 1-9 Load balancer specifications

Parameter	Description
Specifications	<p>Select Elastic or Fixed if pay-per-use is chosen as the billing mode.</p> <ul style="list-style-type: none">• Specification type<ul style="list-style-type: none">– Elastic specifications work well for fluctuating traffic, and you will be charged for how many LCUs you use.– Fixed specifications are suitable for stable traffic, and you will be charged for the specifications you select.• Load balancing type<ul style="list-style-type: none">– Application load balancing (HTTP/HTTPS/QUIC): supports HTTP and HTTPS. This option is a great fit for workloads that require high performance at Layer 7, such as real-time audio and video, interactive livestreaming, and game applications.– Networking load balancing (TCP/UDP/TLS): supports TCP, UDP, and TLS. This option is a great fit for heavy-traffic and high-concurrency workloads at Layer 4, such as file transfer, instant messaging, and online video applications. <p>Select either Application load balancing (HTTP/HTTPS) or Network load balancing (TCP/UDP/TLS) or both, and then select the desired specification. You can select only one specification for Application load balancing (HTTP/HTTPS) and Network load balancing (TCP/UDP/TLS), respectively.</p> <p>Select the desired specifications based on your service size. For details, see Specifications of Dedicated Load Balancers.</p>

4. Complete the network configurations based on [Table 1-10](#).

Table 1-10 Configuring network parameters

Parameter	Description
Network Type	<p>Specifies the network where the load balancer works. You can select one or more network types.</p> <ul style="list-style-type: none">● Private IPv4 network: The load balancer routes IPv4 requests from the clients to backend servers in a VPC. If you want the load balancer to route requests from the Internet, bind an EIP to the load balancer.● IPv6 network: An IPv6 address will be assigned to the load balancer to route requests from IPv6 clients. <p>NOTE If you do not select any option, no IP address will be assigned to the load balancer. If this happens, the load balancer cannot communicate with the clients after it is created. When you are using ELB or testing network connectivity, ensure that the load balancer has a public or private IP address bound.</p>
VPC	<p>Specifies the VPC where the dedicated load balancer works. You cannot change the VPC after the load balancer is created. Plan the VPC as required.</p> <p>Select an existing VPC, or click View VPCs to create a desired one.</p> <p>You can create a load balancer in a VPC subnet shared by another account for improved resource management and reduced O&M costs.</p> <p>For more information about VPC sharing, see VPC Sharing in the Virtual Private Cloud User Guide.</p>
Frontend Subnet	<p>Specifies the frontend subnet from which an IP address will be assigned to the dedicated load balancer to receive client requests.</p> <p>After a load balancer is created, you can unbind the IP address from it and assign an IP address from a new frontend subnet to the load balancer.</p> <p>IP addresses in this subnet will be assigned to load balancers for receiving requests based on the configured network type.</p> <ul style="list-style-type: none">● Private IPv4 network: IPv4 private addresses will be assigned.● IPv6 network: IPv6 private or public addresses will be assigned. <p>NOTE If you select IPv6 network for Network Type and the selected VPC does not have any subnet that supports IPv6, enable IPv6 for at least one subnet or create a subnet that supports IPv6. For details, see the Virtual Private Cloud User Guide.</p>

Parameter	Description
IPv4 Address	<p>Specifies how you want the IPv4 address to be assigned if Network Type is set to Private IPv4 network.</p> <ul style="list-style-type: none">• Automatically assign IP address: The system assigns an IPv4 address to the load balancer.• Manually specify IP address: You need to manually specify an IPv4 address for the load balancer. <p>NOTE Network ACL rules configured for the frontend subnet of a load balancer do not restrict traffic from clients to the load balancer. Use access control to limit which IP addresses can access the load balancer. For details, see What Is Access Control?</p>
Backend Subnet	<p>Specifies the backend subnet from which an IP address will be assigned to the dedicated load balancer to forward requests to backend servers.</p> <ul style="list-style-type: none">• Subnet of the load balancer is selected by default.• Select an existing subnet in the VPC where the load balancer works.• Click Create Subnet on the right to create a new subnet. <p>NOTE</p> <ul style="list-style-type: none">• If you do not enable IPv6 for the specified backend subnet when you create a dedicated load balancer, the load balancer cannot use IPv6 addresses to route requests.• The number of IP addresses required by a load balancer to communicate with the backend servers depends on how many AZs you have selected, how you configure the specifications, and whether you enable the IP as a backend option. See how many IP addresses are actually required on the console.• An application load balancer requires 8 to 30 additional IP addresses in the backend subnet for traffic forwarding. The actual number of required IP addresses depends on the ELB cluster size. If load balancers are deployed in the same cluster and work in the same backend subnet, they share the same IP addresses to save resources.
IPv6 Address	<p>Specifies how you want the IPv6 address to be assigned if Network Type is set to IPv6 network.</p> <ul style="list-style-type: none">• Assign automatically: The system automatically assigns an IPv6 address to the load balancer.• Manually specify: You need to manually specify an IPv6 address for the load balancer. <p>NOTE Network ACL rules configured for the frontend subnet of a load balancer do not restrict traffic from clients to the load balancer. Use access control to limit which IP addresses can access the load balancer. For details, see What Is Access Control?</p>

Parameter	Description
Shared Bandwidth	<p>Specifies the shared bandwidth that the IPv6 address will be added to.</p> <p>A shared bandwidth allows multiple EIPs in the same region to share the same bandwidth.</p> <p>You can choose not to select a shared bandwidth, select an existing shared bandwidth, or buy a shared bandwidth.</p>
IP as a Backend	<p>Specifies whether to associate backend servers that are not in the VPC of the load balancer. After this option is enabled, you can associate the backend servers with the load balancer by using their IP addresses.</p> <p>NOTE</p> <ul style="list-style-type: none">• To use this function, you need to configure correct VPC routes to ensure requests can be routed to backend servers.• If you enable this option, more IP addresses in the backend subnet need to be reserved for the load balancer to communicate with backend servers. Ensure that the selected subnet has sufficient IP addresses. After you select a subnet, you can view the number of IP addresses required by the load balancer in the infotip.

5. Configure an EIP for the load balancer to enable it to route IPv4 requests over the Internet based on [Table 1-11](#).

Table 1-11 Selecting an EIP for the load balancer

Parameter	Description
EIP	<p>Specifies the public IP address that will be bound to the load balancer for receiving and forwarding requests over the Internet.</p> <ul style="list-style-type: none">• Auto assign: A new EIP will be assigned to the load balancer.• Use existing: Select an existing EIP.• Not required: You can bind an EIP to the load balancer later. <p>NOTE</p> <p>If you want to enable a load balancer to communicate with the Internet through a global EIP, you can bind a global EIP to the load balancer.</p>

Parameter	Description
EIP Type	<p>Specifies the link type (BGP) when a new EIP is used.</p> <ul style="list-style-type: none">● Dynamic BGP: If there are changes on a network using dynamic BGP, routing protocols provide automatic, real-time optimization of network configurations, ensuring network stability and optimal user experience. This option works well for workloads that require higher network stability and connectivity, such as financial transactions, online games, large-scale enterprise applications, and livestreaming services.● Static BGP: If there are changes on a network using static BGP, carriers cannot adjust network configurations in real time to ensure optimal user experience. This is a more cost-effective option for workloads that are running in relatively stable networks and have disaster recovery setups.● EIP Pool: assigns EIPs with dynamic BGP routing, ensuring network stability and optimal user experience. <p>For details see What Are the Differences Between Static BGP and Dynamic BGP?</p>
Billed By	<p>Specifies how the bandwidth will be billed.</p> <p>You can select one from the following options:</p> <ul style="list-style-type: none">● Bandwidth: You specify the maximum bandwidth and pay for the amount of time you use the bandwidth.● Traffic: You specify the maximum bandwidth and pay for the outbound traffic you use.● Shared Bandwidth: Load balancers that have EIPs bound in the same region can share the selected bandwidth, helping you reduce public network bandwidth costs.
Bandwidth (Mbit/s)	Specifies the maximum bandwidth.

6. Configure other parameters for the load balancer as described in [Table 1-12](#).

Table 1-12 Configuring other parameters



Parameter	Description
Advanced Settings (Optional) > Description	Click  to expand the configuration area and set this parameter. Enter a description about the load balancer in the text box as required. Enter up to 255 characters. Angle brackets (<>) are not allowed.
Advanced Settings (Optional) > Tag	Click  to expand the configuration area and set this parameter. Add tags to the load balancer so that they can be easily found. A tag consists of a tag key and a tag value. The tag key marks a tag, and the tag value specifies specific tag content. For details about the naming rules, see Table 1-13 . You can add a maximum of 20 tags.

Table 1-13 Tag key and value requirements

Parameter	Requirement
Tag key	<ul style="list-style-type: none">• Cannot be empty.• Must be unique for the same load balancer.• Can contain a maximum of 36 characters.• Can contain only letters, digits, underscores (_), hyphens (-), at signs (@).
Tag value	<ul style="list-style-type: none">• Can contain a maximum of 43 characters.• Can contain only letters, digits, underscores (_), hyphens (-), at signs (@).

7. Select the number of load balancers you want to buy.
8. Click **Buy Now**.

Viewing the Load Balancer Topology

1. Go to the [load balancer list page](#).
2. On the displayed page, click the name of the target load balancer.
The load balancer details page is displayed.
3. Click the **Overview** tab and view the load balancer topology.
The topology displays the listeners and backend server groups associated with the load balancer.
On the topology, you can:

- View the basic information about each listener, and add or edit forwarding policies.
- View the basic information about each backend server group and the backend servers in each group.
- View unhealthy backend servers.

Related Operations

A listener checks requests from clients and routes requests to backend servers using the protocol, port, and load balancing algorithm you select. You need to add at least one listener after you have created a load balancer.

- [Network Listeners](#)
- [Application Listeners](#)
- [Creating a Backend Server Group](#)

Reference

- ELB concepts
 - [What Is ELB?](#)
 - [Feature Comparison Details](#)
 - [Dedicated Load Balancer Overview](#)
- APIs
 - [Creating a Shared Load Balancer](#)
 - [Calculating the Number of Reserved IP Addresses](#)

Popular Questions

- Can ELB Work in a Different AZ from Backend Servers?
Yes. ELB can route requests to backend servers in an AZ that is different from where the load balancer is deployed.
- Can I Change the Specifications of an Existing Load Balancer?
Yes. For details, see [Modifying Specifications](#).

1.3.3 Enabling or Disabling Modification Protection for Dedicated Load Balancers

You can enable modification protection for load balancers to prevent them from being modified or deleted by accident.

Procedure

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
3. Switch to the **Summary** tab and click **Configure** next to **Modification Protection**.
4. In the **Configure Modification Protection** dialog box, enable or disable **Modification Protection**.
Fill in the reason if needed.

5. Click **OK**.

NOTE

You need to disable **Modification Protection** if you want to modify or delete a load balancer.

1.3.4 Modifying the Basic Configurations of a Dedicated Load Balancer

After a dedicated load balancer is created, you can change its specifications and AZ as required.

Modifying Specifications

You can change the specifications of a dedicated load balancer on the console:

- Change the elastic specifications to fixed specifications, or the other way round.
- Change the application load balancing to network load balancing, or the other way round.

You must keep at least one load balancing type. Before removing a load balancing type, you must delete the:

- HTTP, QUIC, or HTTPS listeners added to an application load balancer.
- TCP, TLS, or UDP listeners added to a network load balancer.

- Upgrade or downgrade the fixed specifications, for example, upgrade small I to medium I, or downgrade large I to medium I.

Change options vary by billing mode. To find out what changes you can make, see [Table 1-14](#).

NOTE

- Upgrading specifications does not interrupt your services.
- Downgrading specifications will temporarily disconnect services.
 - Network load balancing (TCP/UDP/TLS): New connections may not be able to be established.
 - Application load balancing (HTTP/HTTPS/QUIC): New connections may not be able to be established and some persistent connections may be interrupted.

Pay-per-Use

Table 1-14 Supported change options for a pay-per-use load balancer

Billing Mode	Specifications	Change to Elastic	Change to Fixed	Add Load Balancing Type	Remove Load Balancing Type	Upgrade Specifications	Downgrade Specifications
Pay-per-use	Elastic	N/A	Supported	Supported	Supported	N/A	N/A

Billing Mode	Specifications	Change to Elastic	Change to Fixed	Add Load Balancing Type	Remove Load Balancing Type	Upgrade Specifications	Downgrade Specifications
	Fixed	Supported	N/A	Supported	Supported	Supported	Supported

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer, click **More** in the **Operation** column, and select **Change Specifications**.
3. Select the new specifications and click **Next**.
4. Confirm the information and click **Submit**.

Changing an AZ

You can change the AZs of a dedicated load balancer as required on the console.

After the AZ is changed, traffic will be distributed to the new AZ.

You can only deploy the load balancer in an additional AZ but cannot remove it from an AZ.

NOTE

This feature will be available in more regions. See details on the management console.

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer, click **More** in the **Operation** column, and select **Change AZs**.
3. Select one or more new AZs and click **Next**.
4. Confirm the information and click **Submit**.

CAUTION

You are advised to change the AZ during off-peak hours. Changing AZs will temporarily affect services. New connections may not be able to be established and some persistent connections may be interrupted.

Popular Questions

Can I Change the Load Balancing Type of a Load Balancer?

Yes, you can change an application load balancer to a network load balancer, or the other way around.

Does Changing Specifications Interrupt Services?

Upgrading specifications does not interrupt your services, but downgrading specifications temporarily does.

1.3.5 Modifying the Network Configurations of a Dedicated Load Balancer

You can change the network configurations of a dedicated load balancer as needed.

Binding or Unbinding an IP Address

You can bind or unbind an IPv4 EIP, a private IPv4 address, or an IPv6 address, to or from a dedicated load balancer as required.

NOTE

- Load balancers without IPv4 EIPs cannot route requests over the public IPv4 network.
- Load balancers without private IPv4 addresses cannot route requests over the private IPv4 network.
- Load balancers without IPv6 addresses cannot route requests over the IPv6 network.
- If you want to enable a load balancer to communicate with the Internet through a global EIP, you can [bind a global EIP to the load balancer](#).

Binding or Unbinding an IPv4 EIP

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click **More** in the **Operation** column.
 - a. Binding an IPv4 EIP
 - i. Click **Bind IPv4 EIP**.
 - ii. In the **Bind IPv4 EIP** dialog box, select the EIP you want to bind to the load balancer and click **OK**.
 - b. Unbinding an IPv4 EIP
 - i. Click **Unbind IPv4 EIP**.
 - ii. In the displayed dialog box, confirm the IPv4 EIP that you want to unbind and click **OK**.

Binding or Unbinding a Private IPv4 Address

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click **More** in the **Operation** column.
 - a. Binding a private IPv4 address
 - i. Click **Bind Private IPv4 Address**.
 - ii. In the **Bind Private IPv4 Address** dialog box, select the subnet where the IP address resides, specify an IP address, and click **OK**.

 NOTE

- By default, an IP address is automatically assigned. To manually specify an IP address, deselect **Automatically assign IP address** and enter an IP address.
 - Ensure that the specified IP address is in the selected subnet and is not in use.
- b. Unbinding a private IPv4 address
 - i. Click **Unbind IPv4 Private IPv4 Address**.
 - ii. In the displayed dialog box, confirm the private IPv4 address that you want to unbind and click **OK**.

Binding or Unbinding an IPv6 Address

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click **More** in the **Operation** column.
 - a. Binding an IPv6 address
 - i. Click **Bind IPv6 Address**.
 - ii. In the **Bind IPv6 Address** dialog box, select the subnet where the IP address resides and click **OK**.
 - b. Unbinding an IPv6 address
 - i. Click **Unbind IPv6 Address**.
 - ii. In the displayed dialog box, confirm the IPv6 address that you want to unbind and click **OK**.

Changing an IP Address

Before changing the private IPv4 address or IPv6 address bound to a dedicated load balancer, note the following:

- The new IPv4 IP address can be in the current subnet or a different subnet.
- The new IPv6 IP address must be in a different subnet with IPv6 enabled.

Changing a Private IPv4 Address

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and choose **More > Change Private IPv4 Address** in the **Operation** column.
3. In the **Change Private IPv4 Address** dialog box, select the subnet where the IP address resides and specify an IP address.
 - To use an IP address in another subnet, if you select **Automatically assign IPv4 address**, an IPv4 address will be assigned to your load balancer.
 - To use another IP address from the current subnet, specify an IP address.
4. Click **OK**.

Changing an IPv6 Address

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and choose **More > Change IPv6 Address** in the **Operation** column.
3. In the **Change IPv6 Address** dialog box, select a different subnet where the IP address resides and specify an IP address.
The system will automatically assign an IPv6 address to the load balancer from the subnet you select.
4. Click **OK**.

Modifying the Bandwidth

If you set the **Network Type** of a load balancer to **Public IPv4 network** or **IPv6 network**, the load balancer can route requests over the Internet and you can modify the bandwidth used by the EIP bound to the load balancer as required. When you modify the bandwidth, traffic routing will not be interrupted.

NOTE

- When modifying bandwidth, you need to change the specifications of the dedicated load balancer to avoid speed limit due to insufficient bandwidth.
 - The EIP bandwidth defines the limit for clients to access the load balancer.
1. Go to the [load balancer list page](#).
 2. On the displayed page, locate the load balancer and click **More** in the **Operation** column.
 3. Click **Modify IPv4 Bandwidth** or **Modify IPv6 Bandwidth**.
 4. In the **New Configuration** area, modify the billing option and bandwidth and click **Next**.
You can select the bandwidth defined by the system or customize a bandwidth. The bandwidth ranges from 1 Mbit/s to 2,000 Mbit/s.
 5. Confirm the new bandwidth and click **Submit**.

NOTE

After you change the billing option and bandwidth, the price will be recalculated accordingly.

Adding or Removing an IPv6 Address to or from a Shared Bandwidth

If the IPv6 address of a load balancer is added to a shared bandwidth, the load balancer can route requests over the Internet.

You can add or remove an IPv6 address to or from a shared bandwidth.

NOTE

- If the IPv6 address of a load balancer is removed from a shared bandwidth, the load balancer can only route requests within a VPC.
1. Go to the [load balancer list page](#).
 2. On the displayed page, locate the load balancer and click **More** in the **Operation** column.

- a. Adding an IPv6 address to a shared bandwidth
 - i. Click **Add to IPv6 Shared Bandwidth**.
 - ii. In the **Add to IPv6 Shared Bandwidth** dialog box, select the shared bandwidth to which you want to add.
If no shared bandwidths are available, assign one as prompted.
 - b. Removing an IPv6 address from a shared bandwidth
 - i. Click **Remove from IPv6 Shared Bandwidth**.
 - ii. In the displayed dialog box, confirm the shared bandwidth you want to remove.
3. Click **OK**.

1.3.6 Exporting Dedicated Load Balancers

Scenarios

You can export the information of all or part of the load balancers under your account as an Excel file to a local directory.

You can export:

- The basic information of all or selected load balancers.
- The details of the selected load balancers.

Basic information includes the name, ID, status, type, and specifications of the load balancers.

Details include basic information of load balancers and listeners by default. In addition, the forwarding policies, backend server groups, backend servers, and certificate name/ID can also be exported.

Exporting the Basic Information of Load Balancers

1. Go to the [load balancer list page](#).
2. Above the load balancer list, click **Export**.
 - a. **Basic information of all resources:** The system automatically exports the basic information of all the load balancers in the current region as an Excel file to a local directory.
 - b. **Basic information of selected resources:** The system automatically exports the basic information of the selected load balancers in the current region as an Excel file to a local directory.

Exporting the Details of Load Balancers

You export the details of selected load balancers, including the associated listeners and backend server groups, forwarding policies, backend servers, and certificates.

1. Go to the [load balancer list page](#).
2. In the upper left corner of the load balancer list, click **Export** and select **Details of selected resources**.
3. In the **Export Resource** dialog box, select the items you want to export.

- a. By default, basic information about load balancers and listeners can be exported.
 - b. You can export forwarding policies, backend server groups, backend servers, or certificate names/IDs.
You can also select **All** to export all information of the selected load balancers.
4. Click **OK**
 5. After the information is exported, click **OK**.

View the Information of the Exported Load Balancers

The system automatically exports the load balancer information as an Excel file to a local directory.

If you export the basic information of load balancers, view the information of each load balancer at each line.

If you export the details of the selected load balancers, view the details of a load balancer at several lines because a load balancer may have more than one listener and backend server group associated with it.

1.3.7 Deleting a Dedicated Load Balancer

Scenarios

You can delete a load balancer if you no longer need it.

⚠ CAUTION

Back up the data if necessary. The data will be deleted immediately after you delete or unsubscribe from the load balancers and cannot be restored.

Notes and Constraints

- If **modification protection** is enabled for a load balancer, you need to disable modification protection on the **Summary** tab of the load balancer before deleting it.
- If **modification protection** is enabled for the listener added to a load balancer, you need to disable modification protection on the **Summary** tab of the listener before deleting the load balancer.
- If **modification protection** is enabled for the backend server group associated with the load balancer, you need to disable modification protection on the **Basic Information** area in the **Summary** tab of the backend server group before deleting the load balancer.

Deleting a Pay-per-Use Load Balancer

After a public network load balancer is deleted, its EIP will not be released and can be used by other resources.

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the target load balancer and choose **More > Delete** in the **Operation** column.
A confirmation dialog box is displayed.
3. Select "Delete the associated backend server groups (If a backend server group is associated with other load balancers, it cannot be deleted.)" if you need.
4. In the displayed dialog box, enter **DELETE**.
5. Click **OK**.

1.3.8 Copying a Dedicated Load Balancer

Overview

After a copy is complete, you will get a new load balancer that has the same basic settings, listeners, and log settings as the original one.

NOTE

This feature is available in certain regions. You can see which regions support them on the console.

Notes and Constraints

- The new load balancer must be in the same VPC as the original one.
- The public network configuration of the original load balancer will not be copied. You can bind an EIP to the new load balancer after the copy is complete.
- Only pay-per-use load balancers can be copied. After the copy is complete, you can change the billing mode of the new load balancer.

Procedure

1. Go to the [load balancer list page](#).
2. Locate the load balancer and click **Copy** in the **Operation** column.
In the **Copy Load Balancer** dialog box, configure parameters for the new load balancer based on [Table 1-15](#).

Table 1-15 Parameters for the new load balancer

Parameter	Description
New Load Balancer Name	Specifies the name of the new load balancer. The name defaults to <i>original load balancer name-copy</i> . You can change it if you want to.

Parameter	Description
AZ	<p>Specifies the AZ of the new load balancer, which defaults to the same AZ as that of the original load balancer. You can change it if you want to.</p> <p>An AZ is a part of a region and has its own independent power supplies and networks. AZs are physically isolated but interconnected through an internal network.</p> <p>For details about AZ planning, see Changing an AZ.</p>
Billing Mode	<p>Specifies the billing mode of the new load balancer. Only Pay-per-use is available.</p>
Specification	<p>Specifies the specifications of the new load balancer. It defaults to the same specifications as the original load balancer, which cannot be changed.</p>
Network Type	<p>Specifies the specifications of the new load balancer. It defaults to the same specifications as the original load balancer, which cannot be changed.</p> <p>The public network configuration of the original load balancer will not be copied. You can bind an EIP to the new load balancer after the copy is complete.</p>
Frontend Subnet	<p>Specifies the frontend subnet of where the new load balancer will work, which defaults to the subnet as that of the original load balancer. You can change it if you want to.</p> <p>A private IP address in this subnet will be assigned to the load balancer to receive client requests.</p>
IPv4 Address	<p>Specifies how you want the IPv4 address to be assigned. There are two options:</p> <ul style="list-style-type: none">• Automatically assign IP address: The system automatically assigns an IPv4 address to the load balancer.• Manually specify IP address: You need to manually specify an IPv4 address to the load balancer.
IPv6 Address	<p>Specifies how you want the IPv6 address to be assigned. If the original load balancer can route IPv6 requests, the new load balancer can too.</p> <p>Automatically assign IP address: The system automatically assigns an IPv6 address to the load balancer.</p>

Parameter	Description
Backend Subnet	<p>Specifies the backend subnet of where the new load balancer will work, which defaults to the subnet as that of the original load balancer. You can change it if you want to.</p> <p>The load balancer uses the IP address in the backend subnet to forward requests to the backend servers.</p> <p>Dedicated load balancers will occupy some IP addresses in the backend subnet. See the number of required IP addresses on the console.</p> <p>If you select a different backend subnet for the new load balancer, ensure that the security group and network ACL rules of backend servers allow traffic from this backend subnet.</p>
Enterprise Project	<p>Specifies an enterprise project by which cloud resources and members are centrally managed.</p> <p>The default project is default.</p>
Backend Server Groups	<p>Specifies whether to reuse or copy a backend server group.</p> <p>If you have enabled enterprise project and use the same project for both the new and original load balancers, you can enable this option.</p> <ul style="list-style-type: none">• Reuse: The backend server groups of the original load balancer will be associated with the new load balancer.• Copy: A new backend server group with the same settings will be created and associated with the new load balancer.

3. Click **OK**.

The copy duration depends on the load balancer settings. In general, each copy completes within 2 minutes.

4. Wait until the copy is complete and click **Close**.

Reference

- [Modifying the Basic Configurations of a Dedicated Load Balancer](#)
- [Modifying the Network Configurations of a Dedicated Load Balancer](#)

1.3.9 Enabling or Disabling a Load Balancer

You can enable or disable a load balancer at any time. The load balancer stops receiving and routing traffic after it is disabled.

If some load balancers are not required but cannot be deleted, you can disable them.

 NOTE

This feature is available in certain regions. You can see which regions support them on the console.

Procedure

1. Go to the [load balancer list page](#).
2. Locate the load balancer and choose **More > Enable** or **More > Disable**.
3. Click **OK**.

 CAUTION

Disabled load balancers will still be billed.

1.4 Listener

1.4.1 Listener Overview

A listener checks requests from clients and routes requests to backend servers using the protocol, port, and load balancing algorithm you select. You need to add at least one listener after you have created a load balancer.

Supported Protocols and Application Scenarios

ELB provides load balancing at both Layer 4 and Layer 7.

You can select TCP, TLS, or UDP for network load balancing and HTTP, QUIC, or HTTPS for application load balancing.

Table 1-16 Protocols supported by ELB

Type	Protocol	Description	Application Scenario
Network listeners	TCP	<ul style="list-style-type: none">• Source IP address-based sticky sessions• Fast data transfer	<ul style="list-style-type: none">• Scenarios that require high reliability and data accuracy, such as file transfer, email, and remote login• Web applications that do not need to handle a large number of concurrent requests and do not require high performance
Network listeners	UDP	<ul style="list-style-type: none">• Relatively low reliability• Fast data transfer	Scenarios that require quick response, such as video chat, gaming, and real-time financial quotations

Type	Protocol	Description	Application Scenario
Network listeners	TLS	<ul style="list-style-type: none">• An extension of HTTP for encrypted data transmission that can prevent unauthorized access• Unidirectional/Bidirectional authentication	Scenarios that require ultra-high performance and large-scale TLS offloading
Application listeners	HTTP	<ul style="list-style-type: none">• Cookie-based sticky sessions• X-Forward-For request header	Applications that require content identification, for example, web applications and mobile games
Application listeners	HTTPS	<ul style="list-style-type: none">• An extension of HTTP for encrypted data transmission that can prevent unauthorized access• Encryption and decryption performed on load balancers• Multiple versions of encryption protocols and cipher suites	Workloads that require encrypted transmission, such as e-commerce and financial services.
Application listeners	QUIC	<ul style="list-style-type: none">• UDP-based low-latency internet transport layer protocol• Multiplexing without head-of-line blocking• Improved congestion control	Applications with a poor network environment and whose users have to switch between networks

 **NOTE**

TLS and QUIC listeners can be created in certain regions. You can see which regions support TLS and QUIC listeners on the console.

Frontend Protocols and Ports

Frontend protocols and ports are used by load balancers to receive requests from clients.

Load balancers use TCP, TLS, or UDP for network load balancing, and HTTP, QUIC, or HTTPS for application load balancing. Select a protocol and a port that best suit your requirements.

NOTE

The frontend protocols and ports cannot be changed once a listener is added. If you want to use a different protocol and port, add another listener.

Table 1-17 Frontend protocols and ports

Frontend Protocol	TCP, UDP, TLS, HTTP, QUIC, or HTTPS
Frontend Port	<p>Listeners using different protocols of a load balancer cannot use the same port. However, UDP listeners can use the same port as listeners that use other protocols. For example, if there is a UDP listener that uses port 88, you can add a TCP listener that also uses port 88. The port number ranges from 1 to 65535.</p> <p>The following are some commonly-used protocols and port numbers:</p> <ul style="list-style-type: none">• TCP/80• HTTPS/443

Backend Protocols and Ports

Backend protocols and ports are used by backend servers to receive requests from load balancers. If Windows servers have Internet Information Services (IIS) installed, the default backend protocol and port are HTTP and 80.

Table 1-18 Backend protocols and ports

Backend Protocol	TCP, UDP, TLS, HTTP, HTTPS, gRPC, or QUIC
Backend Port	<p>Backend servers of a load balancer can use the same ports. The port number ranges from 1 to 65535.</p> <p>The following are some commonly-used protocols and port numbers:</p> <ul style="list-style-type: none">• TCP/80• HTTP/80• HTTPS/443

Forwarding by Port Ranges

Forwarding by Port Ranges is available only when you select TCP or UDP as the frontend protocol.

If this option is enabled, the listener checks requests from all ports in the port range you specify and routes them to the corresponding ports on the backend servers.

Timeout Durations

You can configure and modify timeout durations for your listeners to meet varied demands. For example, if the size of a request from an HTTP or HTTPS client is large, you can prolong the request timeout duration to ensure that the request can be successfully routed.

Figure 1-6 Timeout durations at Layer 4

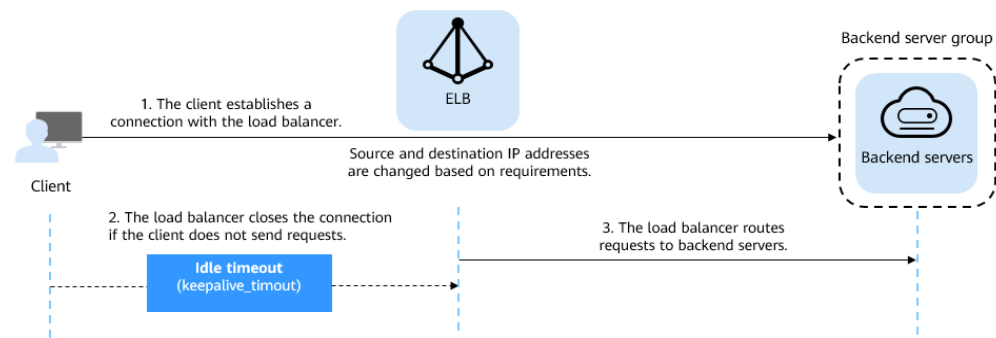


Figure 1-7 Timeout durations at Layer 7

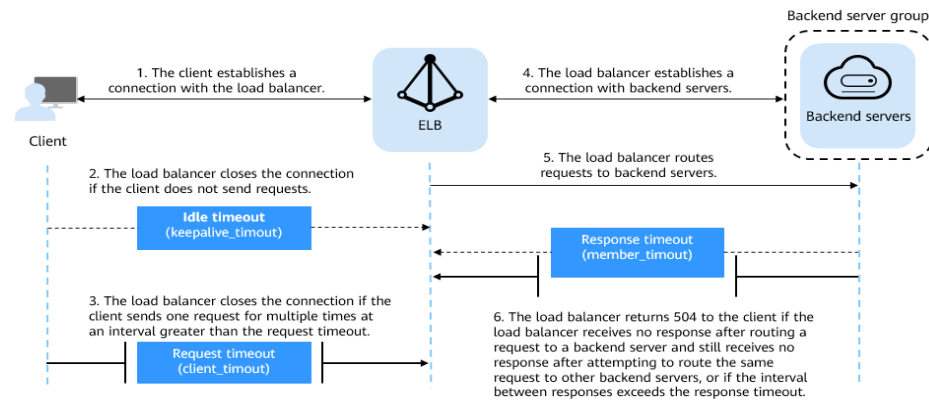


Table 1-19 Timeout durations

Protocol	Type	Description	Value Range	Default Timeout Duration
TCP	Idle Timeout	Duration for a connection to keep alive. If no request is received within this period, the load balancer closes the connection and establishes a new one with the client when the next request arrives.	10–4000s	300s
UDP	Idle Timeout		10–4000s	300s
HTTP/ HTTPS	Idle Timeout		0–4000s	60s
	Request Timeout	Duration that a load balancer is willing to wait for a client request to complete. The load balancer terminates the connection if a request takes too long to complete.	1–300s	60s
	Response Timeout	Duration after which the load balancer sends a 504 Gateway Timeout error to the client if the load balancer receives no response after routing a request to a backend server and receives no response after attempting to route the same request to other backend servers. NOTE If you have enabled sticky sessions and the backend server does not respond within the response timeout duration, the load balancer returns 504 Gateway Timeout to the clients.	1–300s	60s

1.4.2 Network Listeners

1.4.2.1 Adding a TCP Listener

Scenarios

You can add a TCP listener, if high reliability and high accuracy are required but slow speed is acceptable. TCP works well for applications such as file transfer, email sending and receiving, and remote login.

Constraints

- If the front protocol is TCP, the backend protocol defaults to TCP and cannot be changed.
- If you only select the application load balancing type for your dedicated load balancer, you cannot add a TCP listener to this load balancer.

Procedure

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
3. Under **Listeners**, click **Add Listener**. Configure the parameters based on [Table 1-20](#).

Table 1-20 Parameters for configuring a TCP listener

Parameter	Description
Name	Specifies the listener name.
Frontend Protocol	Specifies the protocol that will be used by the load balancer to receive requests from clients. Select TCP .
Forwarding by Port Ranges	This option is available only for TCP or UDP listeners of a dedicated load balancer. It cannot be disabled after it is enabled. If this option is enabled, the listener listens to requests from all ports in the port range you specify and routes the requests to the corresponding ports on the backend servers. NOTE This function is available in certain regions. You can see which regions support this function on the console.
Frontend Port	Specifies the port that will be used by the load balancer to receive requests from clients. The port number ranges from 1 to 65535. NOTE If you enable Forwarding by Port Ranges , you need to enter a start and end port number as the port range.

Parameter	Description
Access Control	Specifies how access to the listener is controlled. For details, see What Is Access Control? The following options are available: <ul style="list-style-type: none">• All IP addresses• Blacklist• Whitelist
IP Address Group	Specifies the IP address group associated with a whitelist or blacklist. If there is no IP address group, create one first. For more information, see IP Address Group .
Transfer Client IP Address	Specifies whether to transmit IP addresses of the clients to backend servers. This function is enabled for dedicated load balancers by default and cannot be disabled.
Advanced Settings	
Idle Timeout	Specifies the length of time for a connection to keep alive, in seconds. If no request is received within this period, the load balancer closes the connection and establishes a new one with the client when the next request arrives. The idle timeout duration ranges from 10 to 4000 .
Maximum New Connections per AZ	Specifies the maximum number of new connections that a listener can handle per second in each AZ. The default value is Unlimited . You can select Limit request to set the maximum number of new connections. The value ranges from 1 to 1000000. If the value is greater than the number defined in the load balancer specifications, the latter is used as the limit. NOTE This option is available in certain regions. You can see which regions support this option on the console.

Parameter	Description
Maximum Concurrent Connections per AZ	<p>Specifies the maximum number of concurrent connections that a listener can handle per second in each AZ. The default value is Unlimited. You can select Limit request to set the maximum number of concurrent connections.</p> <p>The value ranges from 1 to 1000000. If the value is greater than the number defined in the load balancer specifications, the latter is used as the limit.</p> <p>Reducing the concurrent connection limit do not interrupt established connections.</p> <p>NOTE This option is available in certain regions. You can see which regions support this option on the console.</p>
Tag	Adds tags to the listener. Each tag is a key-value pair, and the tag key is unique.
Description	<p>Provides supplementary information about the listener.</p> <p>You can enter a maximum of 255 characters.</p>

4. Click **Next: Configure Request Routing Policy**.
 - a. You are advised to select an existing backend server group.
 - b. You can also click **Create new** to create a backend server group.
 - i. Configure the backend server group based on [Table 1-44](#).
 - ii. Click **Next: Add Backend Server**. Add backend servers and configure health check for the backend server group.

For details about how to add backend servers, see [Backend Server Overview](#). For the parameters required for configuring a health check, see [Table 1-45](#).
5. Click **Next: Confirm**.
6. Confirm the configurations and click **Submit**.

1.4.2.2 Adding a UDP Listener

Scenarios

You can add a UDP listener, if quick response is required but low reliability is acceptable. UDP listeners are suitable for scenarios such as video chat, gaming, and real-time financial quotations.

Constraints

- UDP listeners do not support fragmentation.
- The port of UDP listeners cannot be 4789.

- UDP packets can have any size less than 1,500 bytes. The packets will be discarded if they are bigger than 1,500 bytes. To avoid this, you need to modify the configuration files of the applications based on the maximum transmission unit (MTU) value.
- Dedicated load balancers: The backend protocol can be UDP or QUIC if the frontend protocol is UDP.
- If you only select the application load balancing type for your dedicated load balancer, you cannot add a UDP listener to this load balancer.

Procedure

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
3. Under **Listeners**, click **Add Listener**. Configure the parameters based on [Table 1-21](#).

Table 1-21 Parameters for configuring a UDP listener

Parameter	Description
Name	Specifies the listener name.
Frontend Protocol	Specifies the protocol that will be used by the load balancer to receive requests from clients. Select UDP .
Forwarding by Port Ranges	This option is available only for TCP or UDP listeners of a dedicated load balancer. It cannot be disabled after it is enabled. If this option is enabled, the listener listens to requests from all ports in the port range you specify and routes the requests to the corresponding ports on the backend servers. NOTE This function is available in certain regions. You can see which regions support this function on the console.
Frontend Port	Specifies the port that will be used by the load balancer to receive requests from clients. The port number ranges from 1 to 65535. NOTE If you enable Forwarding by Port Ranges , you need to enter a start and end port number as the port range.
Access Control	Specifies how access to the listener is controlled. For details, see What Is Access Control? The following options are available: <ul style="list-style-type: none">• All IP addresses• Blacklist• Whitelist

Parameter	Description
IP Address Group	Specifies the IP address group associated with a whitelist or blacklist. If there is no IP address group, create one first. For more information, see IP Address Group .
Transfer Client IP Address	Specifies whether to transmit IP addresses of the clients to backend servers. This function is enabled for dedicated load balancers by default and cannot be disabled.
Advanced Settings	
Idle Timeout	Specifies the length of time for a connection to keep alive, in seconds. If no request is received within this period, the load balancer closes the connection and establishes a new one with the client when the next request arrives. The idle timeout duration ranges from 10 to 4000 .
Maximum New Connections per AZ	Specifies the maximum number of new connections that a listener can handle per second in each AZ. The default value is Unlimited . You can select Limit request to set the maximum number of new connections. The value ranges from 1 to 1000000. If the value is greater than the number defined in the load balancer specifications, the latter is used as the limit. NOTE This option is available in certain regions. You can see which regions support this option on the console.
Maximum Concurrent Connections per AZ	Specifies the maximum number of concurrent connections that a listener can handle per second in each AZ. The default value is Unlimited . You can select Limit request to set the maximum number of concurrent connections. The value ranges from 1 to 1000000. If the value is greater than the number defined in the load balancer specifications, the latter is used as the limit. Reducing the concurrent connection limit do not interrupt established connections. NOTE This option is available in certain regions. You can see which regions support this option on the console.
Tag	Adds tags to the listener. Each tag is a key-value pair, and the tag key is unique.

Parameter	Description
Description	Provides supplementary information about the listener. You can enter a maximum of 255 characters.

4. Click **Next: Configure Request Routing Policy**.
 - a. You are advised to select an existing backend server group.
 - b. You can also click **Create new** to create a backend server group.
 - i. Configure the backend server group based on [Table 1-44](#).
 - ii. Click **Next: Add Backend Server**. Add backend servers and configure health check for the backend server group.
For details about how to add backend servers, see [Backend Server Overview](#). For the parameters required for configuring a health check, see [Table 1-45](#).
5. Click **Next: Confirm**.
6. Confirm the configurations and click **Submit**.

1.4.2.3 Adding a UDP Listener (with a QUIC Backend Server Group Associated)

Scenarios

If you use UDP as the frontend protocol, you can select QUIC as the backend protocol, and select the connection ID algorithm to route requests with the same connection ID to the same backend server. QUIC is a great fit for the mobile Internet because it offers low latency, high reliability, and no head-of-line blocking (HOL blocking). Additionally, no new connections need to be established when you switch between a Wi-Fi network and a mobile network.

NOTE

- QUIC versions include Q043, Q046, and Q050.
- UDP listeners using QUIC as backend protocol do not support fragmentation.

Constraints

- Only dedicated load balancers support the QUIC protocol.
- You can add only UDP listeners if you want to use QUIC as the backend protocol.

Procedure

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
Ensure that **Network load balancing (TCP/UDP)** has been selected for the load balancer.
3. Under **Listeners**, click **Add Listener**.

4. In the **Configure Listener** step, set **Frontend Protocol** to **UDP**, configure other parameters as required, and click **Next: Configure Request Routing Policy**.
5. In the **Configure Routing Policy** step, set **Backend Protocol** to **QUIC** and configure other parameters as required.
6. Configure the parameters and click **Submit**.

Related Operations

After you add a listener, associate backend servers with the listener by performing the operations in [Backend Server Overview](#).

1.4.2.4 Adding a TLS Listener

Scenarios

If you require ultra-high performance and large-scale TLS offloading, you can add a TLS listener to forward encrypted TCP requests from clients.

 **NOTE**

TLS is available in certain regions. You can see which regions support TLS on the console.

Constraints

- TLS listeners can only be added to network (TCP/UDP/TLS) load balancers that support new TLS connections.
- TLS listeners can only be associated with TCP or TLS backend server groups.

Procedure

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
3. On the **Listeners** tab, click **Add Listener** and configure parameters based on [Table 1-22](#).

Table 1-22 Parameters for configuring a TLS listener

Parameter	Description
Name	Specifies the listener name.
Frontend Protocol	Specifies the protocol that will be used by the load balancer to receive requests from clients. Select TLS .

Parameter	Description
Forwarding by Port Ranges	<p>This option is available only for TCP, UDP, and TLS listeners of a dedicated load balancer. It cannot be disabled after it is enabled.</p> <p>If this option is enabled, the listener listens to requests from all ports in the port range you specify and routes the requests to the corresponding ports on the backend servers.</p> <p>NOTE If you enable Forwarding by Port Ranges, you need to enter a start and end port number as the port range.</p>
Frontend Port	<p>Specifies the port that will be used by the load balancer to receive requests from clients.</p> <p>The port number ranges from 1 to 65535.</p> <p>NOTE If you enable Forwarding by Port Ranges, you need to enter a start and end port number as the port range.</p>
SSL Authentication	<p>Specifies whether how you want the clients and backend servers to be authenticated.</p> <p>There are two options: One-way authentication or Mutual authentication.</p> <ul style="list-style-type: none">• If only server authentication is required, select One-way authentication.• If you want the clients and the load balancer to authenticate each other, select Mutual authentication. Only authenticated clients will be allowed to access the load balancer.
Server certificate	<p>Specifies the certificate that will be used by the backend server to authenticate the client when TLS is used as the frontend protocol.</p> <p>Both the certificate and private key are required.</p>
CA certificate	<p>Specifies the certificate that will be used by the backend server to authenticate the client when SSL Authentication is set to Mutual authentication.</p> <p>A CA certificate is issued by a certificate authority (CA) and used to verify the certificate issuer. If HTTPS mutual authentication is required, HTTPS connections can be established only when the client provides a certificate issued by a specific CA.</p>

Parameter	Description
Enable SNI	<p>Specifies whether to enable SNI when TLS is used as the frontend protocol.</p> <p>SNI is an extension to TLS and is used when a server uses multiple domain names and certificates.</p> <p>This allows the client to submit the domain name information while sending an SSL handshake request. After the load balancer receives the request, the load balancer queries the corresponding certificate based on the domain name and returns it to the client. If no certificate is found, the load balancer will return the default certificate. For details, see SNI Certificate.</p>
SNI Certificate	<p>Specifies the certificate associated with the domain name when the frontend protocol is HTTPS and SNI is enabled.</p> <p>Select an existing certificate or create one.</p>
Access Control	<p>Specifies how access to the listener is controlled. For details, see What Is Access Control? The following options are available:</p> <ul style="list-style-type: none">• All IP addresses• Blacklist• Whitelist
IP Address Group	<p>Specifies the IP address group associated with a whitelist or blacklist. If there is no IP address group, create one first. For more information, see IP Address Group.</p>
Transfer Client IP Address	<p>If the frontend protocol is TLS, the source IP addresses of the clients cannot be passed to backend servers. Enable ProxyProtocol to transfer the source IP addresses.</p>
ProxyProtocol	<p>Specifies whether to enable the ProxyProtocol option to pass the source IP addresses of the clients to backend servers.</p> <p>NOTE Ensure the backend servers support ProxyProtocol. Otherwise, services may be interrupted.</p>
Advanced Settings	
Security Policy	<p>Specifies the security policy you can use if you select TLS as the frontend protocol. For more information, see TLS Security Policy.</p>

Parameter	Description
Idle Timeout	<p>Specifies the length of time for a connection to keep alive, in seconds. If no request is received within this period, the load balancer closes the connection and establishes a new one with the client when the next request arrives.</p> <p>The idle timeout duration ranges from 0 to 4000.</p>
Maximum New Connections per AZ	<p>Specifies the maximum number of new connections that a listener can handle per second in each AZ. The default value is Unlimited. You can select Limit request to set the maximum number of new connections.</p> <p>The value ranges from 1 to 1000000. If the value is greater than the number defined in the load balancer specifications, the latter is used as the limit.</p> <p>NOTE This option is available in certain regions. You can see which regions support this option on the console.</p>
Maximum Concurrent Connections per AZ	<p>Specifies the maximum number of concurrent connections that a listener can handle per second in each AZ. The default value is Unlimited. You can select Limit request to set the maximum number of concurrent connections.</p> <p>The value ranges from 1 to 1000000. If the value is greater than the number defined in the load balancer specifications, the latter is used as the limit.</p> <p>Reducing the concurrent connection limit do not interrupt established connections.</p> <p>NOTE This option is available in certain regions. You can see which regions support this option on the console.</p>
Tag	<p>Adds tags to the listener. Each tag is a key-value pair, and the tag key is unique.</p>
Description	<p>Provides supplementary information about the listener.</p> <p>You can enter a maximum of 255 characters.</p>

4. Click **Next: Configure Request Routing Policy**.
 - a. You are advised to select an existing backend server group.
 - b. You can also click **Create new** to create a backend server group.
 - i. Configure the backend server group based on [Table 1-44](#).
 - ii. Click **Next: Add Backend Server**. Add backend servers and configure the health check for the backend server group.

For details about how to add backend servers, see [Backend Server Overview](#). For the parameters required for configuring a health check, see [Table 1-45](#).

5. Click **Next: Confirm**.
6. Confirm the configuration and click **Submit**.

1.4.3 Application Listeners

1.4.3.1 Adding an HTTP Listener

Scenarios

You can add an HTTP listener if content identification is required. HTTP is a great fit for workloads such as web applications and mobile mini-games.

Constraints

- If the listener protocol is HTTP, the backend protocol is HTTP by default and cannot be changed.
- If you only select the network load balancing type for your dedicated load balancer, you cannot add an HTTP listener to this load balancer.

Procedure

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
3. Under **Listeners**, click **Add Listener**. Configure the parameters based on [Table 1-23](#).

Table 1-23 Parameters for configuring an HTTP listener

Parameter	Description
Name	Specifies the listener name.
Frontend Protocol	Specifies the protocol that will be used by the load balancer to receive requests from clients. Select HTTP .
Frontend Port	Specifies the port that will be used by the load balancer to receive requests from clients. The port number ranges from 1 to 65535.

Parameter	Description
Redirect	<p>Specifies whether to enable redirection.</p> <p>If you have both HTTPS and HTTP listeners, you can use this function to redirect the requests from an HTTP listener to an HTTPS listener to ensure security.</p> <p>After the redirection is added for an HTTP listener, the backend server will return 301 Moved Permanently to the clients.</p>
Redirected To	<p>Specifies the HTTPS listener to which requests are redirected if Redirect is enabled.</p>
Access Control	<p>Specifies how access to the listener is controlled. For details, see What Is Access Control? The following options are available:</p> <ul style="list-style-type: none">• All IP addresses• Blacklist• Whitelist
IP Address Group	<p>Specifies the IP address group associated with a whitelist or blacklist. If there is no IP address group, create one first. For more information, see IP Address Group.</p>
Transfer Client IP Address	<p>Specifies whether to transmit IP addresses of the clients to backend servers.</p> <p>This function is enabled for dedicated load balancers by default and cannot be disabled.</p>
Advanced Forwarding	<p>Specifies whether to enable the advanced forwarding policy. You can configure advanced forwarding policies for HTTP or HTTPS listeners to forward requests to different backend server groups.</p> <p>For more information, see Advanced Forwarding.</p>
Advanced Settings	

Parameter	Description
HTTP Headers	<p>You can enable the following options as needed.</p> <ul style="list-style-type: none"> ● Transfer headers: <ul style="list-style-type: none"> – Transfer Load Balancer EIP: transmits the EIP bound to the load balancer to backend servers through the X-Forwarded-ELB-IP header. – Transfer Listener Port Number: transmits the port number used by the listener to backend servers through the X-Forwarded-Port header. – Transfer Port Number in the Request: transmits the port number used by the client to backend servers through the X-Forwarded-For-Port header. – Transfer Load Balancer ID: transmits the load balancer ID to backend servers through the X-Forwarded-ELB-ID header. ● Rewrite headers: <ul style="list-style-type: none"> – Rewrite X-Forwarded-Host: rewrites the Host header of the client into the X-Forwarded-Host header and transmits it to the backend servers. – Rewrite X-Forwarded-Proto: rewrites the listener protocol into the X-Forwarded-Proto header and transmits it to the backend servers. – Rewrite X-Real-IP: rewrites the source IP address of the client into the X-Real-IP header and transmits it to the backend servers. <p>For details, see HTTP Headers.</p> <p>NOTE More HTTP headers are coming soon. See the available HTTP headers on the management console.</p>
Data Compression	<p>Specifies whether to enable the data compression option. If you do not enable this option, files will not be compressed.</p> <ul style="list-style-type: none"> ● Brotli can compress all files. ● Gzip can be configured to compress the following content types: text/xml text/plain text/css application/javascript application/x-javascript application/rss+xml application/atom+xml application/xml application/json. <p>NOTE This option is available in certain regions. You can see which regions support this option on the console.</p>

Parameter	Description
Idle Timeout (s)	<p>Specifies the length of time for a connection to keep alive, in seconds. If no request is received within this period, the load balancer closes the connection and establishes a new one with the client when the next request arrives.</p> <p>The idle timeout duration ranges from 0 to 4000.</p>
Request Timeout (s)	<p>Specifies the length of time (in seconds) that a load balancer is willing to wait for a client request to complete. The load balancer terminates the connection if a request takes too long to complete.</p> <p>The request timeout duration ranges from 1 to 300.</p>
Response Timeout (s)	<p>Specifies the length of time (in seconds) after which the load balancer sends a 504 Gateway Timeout error to the client if the load balancer receives no response from the backend server after routing a request to the backend server and receives no response after attempting to route the same request to other backend servers.</p> <p>The response timeout duration ranges from 1 to 300.</p> <p>NOTE If you have enabled sticky sessions and the backend server does not respond within the response timeout duration, the load balancer returns 504 Gateway Timeout to the clients.</p>
Maximum New Connections per AZ	<p>Specifies the maximum number of new connections that a listener can handle per second in each AZ. The default value is Unlimited. You can select Limit request to set the maximum number of new connections.</p> <p>The value ranges from 1 to 1000000. If the value is greater than the number defined in the load balancer specifications, the latter is used as the limit.</p> <p>NOTE This option is available in certain regions. You can see which regions support this option on the console.</p>

Parameter	Description
Maximum Concurrent Connections per AZ	<p>Specifies the maximum number of concurrent connections that a listener can handle per second in each AZ. The default value is Unlimited. You can select Limit request to set the maximum number of concurrent connections.</p> <p>The value ranges from 1 to 1000000. If the value is greater than the number defined in the load balancer specifications, the latter is used as the limit.</p> <p>Reducing the concurrent connection limit do not interrupt established connections.</p> <p>NOTE This option is available in certain regions. You can see which regions support this option on the console.</p>
Tag	<p>Adds tags to the listener. Each tag is a key-value pair, and the tag key is unique.</p> <p>NOTE This option is available in certain regions. You can see which regions support this option on the console.</p>
Description	<p>Provides supplementary information about the listener.</p> <p>You can enter a maximum of 255 characters.</p>

4. Click **Next: Configure Request Routing Policy**.
 - a. You are advised to select an existing backend server group.
 - b. You can also click **Create new** to create a backend server group.
 - i. Configure the backend server group based on [Table 1-44](#).
 - ii. Click **Next: Add Backend Server**. Add backend servers and configure health check for the backend server group.

For details about how to add backend servers, see [Backend Server Overview](#). For the parameters required for configuring a health check, see [Table 1-45](#).
5. Click **Next: Confirm**.
6. Confirm the configurations and click **Submit**.

1.4.3.2 Adding an HTTPS Listener

Scenarios

You can add an HTTPS listener if you require encrypted transmission. Load balancers decrypt HTTPS requests before routing them to backend servers. Once the servers process the requests, they send them back to the load balancers for encryption. Finally, the load balancers send the encrypted requests to the clients.

When you add an HTTPS listener, ensure that the subnet of the load balancer has sufficient IP addresses. If the IP addresses are insufficient, add more subnets on

the summary page of the load balancer. After you select a subnet, ensure that ACL rules are not configured for this subnet. If rules are configured, request packets may not be allowed.

Constraints

- If the listener protocol is HTTPS, the backend protocol can be HTTP or HTTPS.
- If you only select the network load balancing type for your dedicated load balancer, you cannot add an HTTPS listener to this load balancer.

Procedure

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
3. Under **Listeners**, click **Add Listener**. Configure the parameters based on [Table 1-24](#).

Table 1-24 Parameters for configuring an HTTPS listener

Parameter	Description
Name	Specifies the listener name.
Frontend Protocol	Specifies the protocol that will be used by the load balancer to receive requests from clients. Select HTTPS .
Frontend Port	Specifies the port that will be used by the load balancer to receive requests from clients. The port number ranges from 1 to 65535.
SSL Authentication	Specifies how you want the clients and backend servers to be authenticated. There are two options: One-way authentication or Mutual authentication . <ul style="list-style-type: none">• If only server authentication is required, select One-way authentication.• If you want the clients and the load balancer to authenticate each other, select Mutual authentication. Only authenticated clients will be allowed to access the load balancer.
CA Certificate	Specifies the certificate that will be used by the backend server to authenticate the client when SSL Authentication is set to Mutual authentication . A CA certificate is issued by a certificate authority (CA) and used to verify the certificate issuer. If HTTPS mutual authentication is required, HTTPS connections can be established only when the client provides a certificate issued by a specific CA. For details, see Adding a Certificate .

Parameter	Description
Server Certificate	<p>Specifies the certificate that will be used by the backend server to authenticate the client when HTTPS is used as the frontend protocol.</p> <p>The server certificate is used for SSL handshake negotiation to authenticate clients and ensure encrypted transmission.</p> <p>For details, see Adding a Certificate.</p>
Enable SNI	<p>Specifies whether to enable SNI when HTTPS is used as the frontend protocol. SNI can be used when a server uses multiple domain names and certificates.</p> <p>This allows the client to submit the domain name information while sending an SSL handshake request. After the load balancer receives the request, the load balancer queries the corresponding certificate based on the domain name and returns it to the client. If no certificate is found, the load balancer will return the default certificate. For details, see SNI Certificate.</p>
SNI Certificate	<p>Specifies the certificate associated with the domain name when the frontend protocol is HTTPS and SNI is enabled.</p> <p>Select an existing certificate or create one.</p> <p>For details, see Adding a Certificate.</p>
Access Control	<p>Specifies how access to the listener is controlled. For details, see What Is Access Control? The following options are available:</p> <ul style="list-style-type: none">• All IP addresses• Blacklist• Whitelist
IP Address Group	<p>Specifies the IP address group associated with a whitelist or blacklist. If there is no IP address group, create one first. For more information, see IP Address Group.</p>
Transfer Client IP Address	<p>Specifies whether to transmit IP addresses of the clients to backend servers.</p> <p>This function is enabled for dedicated load balancers by default and cannot be disabled.</p>
Advanced Forwarding	<p>Specifies whether to enable the advanced forwarding policy. You can configure advanced forwarding policies for HTTP or HTTPS listeners to forward requests to different backend server groups.</p> <p>For more information, see Advanced Forwarding.</p>

Parameter	Description
Advanced Settings	
Security Policy	Specifies the security policy you can use if you select HTTPS as the frontend protocol. For more information, see TLS Security Policy .
HTTP/2	Specifies whether you want to use HTTP/2 if you select HTTPS for Frontend Protocol . For details, see HTTP/2 .
HTTP Headers	<p>You can enable the following options as needed.</p> <ul style="list-style-type: none">• Transfer headers:<ul style="list-style-type: none">– Transfer Load Balancer EIP: transmits the EIP bound to the load balancer to backend servers through the X-Forwarded-ELB-IP header.– Transfer Listener Port Number: transmits the port number used by the listener to backend servers through the X-Forwarded-Port header.– Transfer Port Number in the Request: transmits the port number used by the client to backend servers through the X-Forwarded-For-Port header.– Transfer Load Balancer ID: transmits the load balancer ID to backend servers through the X-Forwarded-ELB-ID header.• Rewrite headers:<ul style="list-style-type: none">– Rewrite X-Forwarded-Host: rewrites the Host header of the client into the X-Forwarded-Host header and transmits it to the backend servers.– Rewrite X-Forwarded-Proto: rewrites the listener protocol into the X-Forwarded-Proto header and transmits it to the backend servers.– Rewrite X-Real-IP: rewrites the source IP address of the client into the X-Real-IP header and transmits it to the backend servers. <p>For details, see HTTP Headers.</p> <p>NOTE More HTTP headers are coming soon. See the available HTTP headers on the management console.</p>

Parameter	Description
Data Compression	<p>Specifies whether to enable the data compression option. If you do not enable this option, files will not be compressed.</p> <ul style="list-style-type: none">• Brotli can compress all files.• Gzip can be configured to compress the following content types: text/xml text/plain text/css application/javascript application/x-javascript application/rss+xml application/atom+xml application/xml application/json. <p>NOTE This option is available in certain regions. You can see which regions support this option on the console.</p>
Idle Timeout (s)	<p>Specifies the length of time for a connection to keep alive, in seconds. If no request is received within this period, the load balancer closes the connection and establishes a new one with the client when the next request arrives.</p> <p>The idle timeout duration ranges from 0 to 4000.</p>
Request Timeout (s)	<p>Specifies the length of time (in seconds) that a load balancer is willing to wait for a client request to complete. The load balancer terminates the connection if a request takes too long to complete.</p> <p>The request timeout duration ranges from 1 to 300.</p>
Response Timeout (s)	<p>Specifies the length of time (in seconds) after which the load balancer sends a 504 Gateway Timeout error to the client if the load balancer receives no response from the backend server after routing a request to the backend server and receives no response after attempting to route the same request to other backend servers.</p> <p>The response timeout duration ranges from 1 to 300.</p> <p>NOTE If you have enabled sticky sessions and the backend server does not respond within the response timeout duration, the load balancer returns 504 Gateway Timeout to the clients.</p>

Parameter	Description
Maximum New Connections per AZ	<p>Specifies the maximum number of new connections that a listener can handle per second in each AZ. The default value is Unlimited. You can select Limit request to set the maximum number of new connections.</p> <p>The value ranges from 1 to 1000000. If the value is greater than the number defined in the load balancer specifications, the latter is used as the limit.</p> <p>NOTE This option is available in certain regions. You can see which regions support this option on the console.</p>
Maximum Concurrent Connections per AZ	<p>Specifies the maximum number of concurrent connections that a listener can handle per second in each AZ. The default value is Unlimited. You can select Limit request to set the maximum number of concurrent connections.</p> <p>The value ranges from 1 to 1000000. If the value is greater than the number defined in the load balancer specifications, the latter is used as the limit.</p> <p>Reducing the concurrent connection limit do not interrupt established connections.</p> <p>NOTE This option is available in certain regions. You can see which regions support this option on the console.</p>
Tag	<p>Adds tags to the listener. Each tag is a key-value pair, and the tag key is unique.</p> <p>NOTE This option is available in certain regions. You can see which regions support this option on the console.</p>
Description	<p>Provides supplementary information about the listener.</p> <p>You can enter a maximum of 255 characters.</p>

4. Click **Next: Configure Request Routing Policy**.
 - a. You are advised to select an existing backend server group.
 - b. You can also click **Create new** to create a backend server group.
 - i. For details about how to configure a backend server group, see [Table 1-44](#).
 - ii. Click **Next: Add Backend Server**. Add backend servers and configure health check for the backend server group.

For details about how to add backend servers, see [Backend Server Overview](#). For the parameters required for configuring a health check, see [Table 1-45](#).

5. Click **Next: Confirm**.
6. Confirm the configurations and click **Submit**.

1.4.3.3 Adding a QUIC Listener

Scenarios

You can add a QUIC listener to forward requests. The Quick UDP Internet Connection (QUIC) is a UDP-based protocol at the transport layer. It improves congestion control and does not depend on kernel protocols.

QUIC features low latency and avoids head-of-line blocking. It makes video and page loading faster, improving network performance and data security.

Constraints

- QUIC listeners can be only added to application load balancers.

 **NOTE**

QUIC listeners will be available in more regions. See details on the management console.

- QUIC listeners can only be associated with HTTP or HTTPS backend server groups.
- Only iQUIC (HTTP/3) is supported.

Adding a QUIC Listener

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
3. On the **Listeners** tab, click **Add Listener** and configure parameters based on [Table 1-25](#).

Table 1-25 Parameters for configuring a QUIC listener

Parameter	Description
Name	Specifies the listener name.
Frontend Protocol	Specifies the protocol that will be used by the load balancer to receive requests from clients.
Frontend Port	Specifies the port that will be used by the load balancer to receive requests from clients. The port number ranges from 1 to 65535.
SSL Authentication	Specifies whether how you want the clients and backend servers to be authenticated. QUIC listeners support only one-way authentication on the server.

Parameter	Description
Server certificate	<p>Specifies the certificate that will be used by the backend server to authenticate the client when QUIC is used as the frontend protocol.</p> <p>Both the certificate and private key are required. For details, see Adding a Certificate.</p>
Enable SNI	<p>Specifies whether to enable SNI when QUIC is used as the frontend protocol.</p> <p>SNI is an extension to TLS and is used when a server uses multiple domain names and certificates.</p> <p>This allows the client to submit the domain name information while sending an SSL handshake request. After the load balancer receives the request, the load balancer queries the corresponding certificate based on the domain name and returns it to the client. If no certificate is found, the load balancer will return the default certificate. For details, see SNI Certificate.</p>
SNI Certificate	<p>Specifies the certificate associated with the domain name when the frontend protocol is HTTPS and SNI is enabled.</p> <p>Select an existing certificate or create one. For details, see Adding a Certificate.</p>
Access Control	<p>Specifies how access to the listener is controlled. For details, see What Is Access Control? The following options are available:</p> <ul style="list-style-type: none">• All IP addresses• Blacklist• Whitelist
Transfer Client IP Address	<p>Specifies whether to transmit IP addresses of the clients to backend servers.</p> <p>This function is enabled for dedicated load balancers by default and cannot be disabled.</p>
Advanced Forwarding	<p>Specifies whether to enable the advanced forwarding policy. You can configure advanced forwarding policies for HTTP or HTTPS listeners to forward requests to different backend server groups.</p> <p>For more information, see Advanced Forwarding.</p>
Advanced Settings	

Parameter	Description
HTTP Headers	<p>You can enable the following options as needed.</p> <ul style="list-style-type: none">• Transfer headers:<ul style="list-style-type: none">– Transfer Load Balancer EIP: transmits the EIP bound to the load balancer to backend servers through the X-Forwarded-ELB-IP header.– Transfer Listener Port Number: transmits the port number used by the listener to backend servers through the X-Forwarded-Port header.– Transfer Load Balancer ID: transmits the load balancer ID to backend servers through the X-Forwarded-ELB-ID header.• Rewrite headers:<ul style="list-style-type: none">– Rewrite X-Forwarded-Host: rewrites the Host header of the client into the X-Forwarded-Host header and transmits it to the backend servers.– Rewrite X-Forwarded-Proto: rewrites the listener protocol into the X-Forwarded-Proto header and transmits it to the backend servers. <p>For details, see HTTP Headers.</p>
Data Compression	<p>Specifies whether to enable the data compression option. If you do not enable this option, files will not be compressed.</p> <ul style="list-style-type: none">• Brotli can compress all files.• Gzip can be configured to compress the following content types: text/xml text/plain text/css application/javascript application/x-javascript application/rss+xml application/atom+xml application/xml application/json. <p>NOTE This option is available in certain regions. You can see which regions support this option on the console.</p>

Parameter	Description
Timeout Durations	<p>You can configure and modify timeout durations for your listeners to meet varied demands.</p> <ul style="list-style-type: none"> ● Idle Timeout (s) Specifies the length of time for a connection to keep alive, in seconds. If no request is received within this period, the load balancer closes the connection and establishes a new one with the client when the next request arrives. The idle timeout duration ranges from 0 to 4000. ● Request Timeout (s) Specifies the length of time (in seconds) that a load balancer is willing to wait for a client request to complete. The load balancer terminates the connection if a request takes too long to complete. The request timeout duration ranges from 1 to 300. ● Response Timeout (s) Specifies the length of time (in seconds) after which the load balancer sends a 504 Gateway Timeout error to the client if the load balancer receives no response from the backend server after routing a request to the backend server and receives no response after attempting to route the same request to other backend servers. The response timeout duration ranges from 1 to 300. <p>NOTE If sticky sessions are enabled and the backend server does not respond within the response timeout duration, the load balancer returns the 504 error code without attempting to route the same request to other backend servers.</p>
Maximum New Connections per AZ	<p>Specifies the maximum number of new connections that a listener can handle per second in each AZ. The default value is Unlimited. You can select Limit request to set the maximum number of new connections.</p> <p>The value ranges from 1 to 1000000. If the value is greater than the number defined in the load balancer specifications, the latter is used as the limit.</p> <p>NOTE This option is available in certain regions. You can see which regions support this option on the console.</p>

Parameter	Description
Maximum Concurrent Connections per AZ	<p>Specifies the maximum number of concurrent connections that a listener can handle per second in each AZ. The default value is Unlimited. You can select Limit request to set the maximum number of concurrent connections.</p> <p>The value ranges from 1 to 1000000. If the value is greater than the number defined in the load balancer specifications, the latter is used as the limit.</p> <p>Reducing the concurrent connection limit do not interrupt established connections.</p> <p>NOTE This option is available in certain regions. You can see which regions support this option on the console.</p>
Tag	<p>Adds tags to the listener. Each tag is a key-value pair, and the tag key is unique.</p> <p>NOTE If your organization has configured tag policies for ELB, add tags to load balancers based on the tag policies. If you add a tag that does not comply with the tag policies, load balancers may fail to be created. Contact your organization administrator to learn more about tag policies.</p>
Description	<p>Provides supplementary information about the listener.</p> <p>You can enter a maximum of 255 characters.</p>

4. Click **Next: Configure Request Routing Policy**.
 - a. You are advised to select an existing backend server group.
 - b. You can also click **Create new** to create a backend server group.
 - i. Configure the backend server group based on [Table 1-44](#).
 - ii. Click **Next: Add Backend Server**. Add backend servers and configure the health check for the backend server group.

For details about how to add backend servers, see [Backend Server Overview](#). For the parameters required for configuring a health check, see [Table 1-45](#).
5. Click **Next: Confirm**.
6. Confirm the configuration and click **Submit**.

1.4.3.4 Forwarding Policy

Overview

You can configure forwarding policies for HTTP or HTTPS listeners to forward requests to different backend server groups based on domain names or paths.

A forwarding policy consists of two parts: forwarding rule and action. For details, see [Table 1-26](#).

Table 1-26 Rules and actions supported by a forwarding policy

Policy Type	Forwarding Rules	Actions
Forwarding policy	Domain name and Path	Forward to another backend server group and Redirect to another listener (only for HTTP listeners)
Advanced forwarding policy	Domain name, Path, HTTP request method, HTTP header, Query string, and CIDR block	Forward to another backend server group, Redirect to another listener, Rewrite, Write header, Remove header, Limit request, and Return a specific response body

 **NOTE**

You can configure an advanced forwarding policy by referring to [Managing an Advanced Forwarding Policy](#).

How Requests Are Matched

- After receiving a request, the load balancer attempts to find a matching forwarding policy based on the domain name or path in the request:
 - If a match is found, the request is forwarded to the backend server group you select or create when you add the forwarding policy.
 - If no match is found, the request is forwarded to the default backend server group that is specified when the listener is created.
 - If both a domain name and path are configured for a forwarding policy, the request can match the forwarding policy only when the domain name and path are both met.
- If advanced forwarding is not enabled for a dedicated load balancer, the matching order is determined by the following rules:
 - When a request matches both a domain name-based policy and a path-based policy, the domain named-based policy is matched first. [Table 1-27](#) shows an example.
 - Forwarding policy priorities are independent of each other regardless of domain names.
 - Path-based forwarding rules are applied in the following order of priority: an exact match rule, a prefix match rule, and a regular expression match rule. For multiple matches of the same type, only the longest path rule will be applied.

Table 1-27 Example forwarding policies

Request	Forwarding Policy	Forwarding Rule	Specified Value
www.elb.com/ test	1	Path	/test
	2	Domain name	www.elb.com

NOTE

In this example, although request **www.elb.com/test** matches both forwarding policies, it is routed based on forwarding policy 2 because domain named-based forwarding rules are applied first.

Notes and Constraints

- Forwarding policies can be configured only for HTTP and HTTPS listeners.
- Forwarding policies must be unique.
- A maximum of 100 forwarding policies can be configured for a listener. If the number of forwarding policies exceeds the quota, the excess forwarding policies will not be applied.
- When you add a forwarding policy, note the following:
 - The URL in a forwarding rule can contain only a path but cannot contain query strings. For example, if the path is set to **/path/resource?name=value**, the forwarding policy is invalid.
 - Each path must exist on the backend server. If the path does not exist, the backend server will return 404 Not Found.
 - In the regular expression match, the characters are matched sequentially, and the matching ends when any rule is matched. Matching rules cannot overlap with each other.
 - A path cannot be configured for two forwarding policies.
 - A domain name cannot exceed 100 characters.

Adding a Forwarding Policy

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer you want to add forwarding policy for and click its name.
3. On the **Listeners** tab, add a forwarding policy in either of the following ways:
 - Locate the target listener and click **Add/Edit Forwarding Policy** in the **Forwarding Policies** column.
 - Locate the target listener, click its name, and click the **Forwarding Policies** tab.
4. Click **Add Forwarding Policy**. Configure the parameters based on [Table 1-28](#).

Table 1-28 Forwarding policy parameters

Parameter	Type	Description	Example Value
Forwarding Rule	Domain name	Specifies the domain name that will be exactly matched against the domain names in requests. You need to specify either a domain name or path.	www.test.com
	Path	<ul style="list-style-type: none">• Description Specifies the path used for forwarding requests. A path can contain letters, digits, and special characters: _~';@^-%#\$.*+?,=:\ /()[]{} • Matching rules<ul style="list-style-type: none">- Exact match: The request path is the same as the specified path and must start with a slash (/).- Prefix match: The request path starts with the specified path string and must start with a slash (/).- Regular expression match: The paths are matched using a regular expression.	/login.php
Action	Forward to a backend server group	Specifies the backend server group to which a request is routed if it matches the configured forwarding rule.	N/A
	Redirect to another listener	Specifies the HTTPS listener to which a request is routed if it matches the configured forwarding rule. This action can be configured only for HTTP listeners. NOTE If you select Redirect to another listener , the HTTP listener will redirect requests to the specified HTTPS listener, but access control configured for the HTTP listener still takes effect.	N/A

5. Click **Save**.

1.4.3.5 Advanced Forwarding

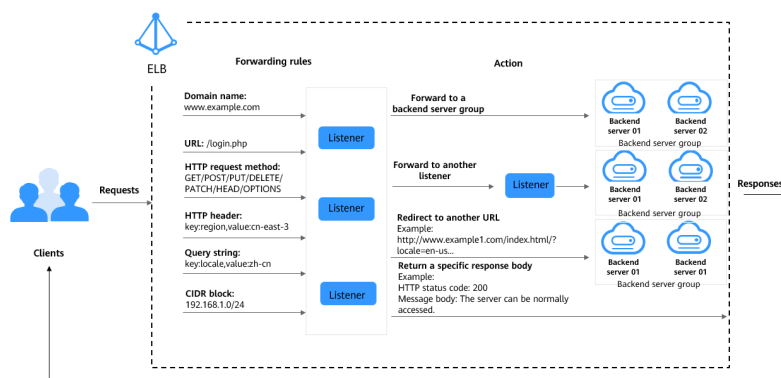
1.4.3.5.1 Advanced Forwarding

Overview

Advanced forwarding policies are available only for dedicated load balancers. If you have enabled **Advanced Forwarding**, you can configure advanced forwarding policies for HTTP and HTTPS listeners of dedicated load balancers.

You can configure advanced forwarding policies for HTTP or HTTPS listeners to forward requests to different backend server groups based on a wide range of forwarding rules and actions. [Table 1-29](#) describes the rules and actions that you can configure for request forwarding.

Figure 1-8 How advanced forwarding works



The following describes how an advanced forwarding policy works:

- Step 1** The client sends a request to the load balancer.
- Step 2** The load balancer matches the request based on the forwarding rule you configure.
- Step 3** The load balancer forwards the request to the corresponding backend server or returns a fixed response to the client based on the action you configure.
- Step 4** The load balancer sends a response to the client.

----End

Table 1-29 Rules and actions supported by an advanced forwarding policy

Forwarding Policy	Description
Forwarding rule	The following forwarding rules are supported: domain name, path, HTTP request method, HTTP header, query string, cookie, and CIDR block. For details, see Forwarding Rule .

Forwarding Policy	Description
Action	<p>The following actions are supported: forward to a backend server group, redirect to another listener, redirect to another URL, rewrite, write header, remove header, limit request, and return a specific response body.</p> <p>NOTE</p> <ul style="list-style-type: none">• If Action is set to Forward to a backend server group, you can also select from one of the following additional actions: rewrite, write header, remove header, and limit request.• If Action is set to Return a specific response body, you can also select the additional action Limit request. <p>For details, see Table 1-32.</p> <p>For details, see Action Types.</p>

 **NOTE**

These additional actions are only available in certain regions. You can check which regions support these actions on the console. If you want to use these actions, [submit a service ticket](#).

How Requests Are Matched

After you add an HTTP or HTTPS listener to a load balancer, a default forwarding policy is generated. This policy uses the protocol and port specified for the listener to match requests and forward the requests to the backend server group you specified when adding the listener.

The default forwarding policy has the lowest priority and is not included when you sort forwarding policies. It can be edited but cannot be deleted.

Each request is matched based on the forwarding policy priority (a smaller value indicates a higher priority). Once a forwarding policy is matched, the request is forwarded based on this forwarding policy.

- If multiple conditions are configured for a forwarding policy, the request can match this forwarding policy only when all the conditions are met.
- If the request is matched with any forwarding policy of the listener, it is forwarded based on this forwarding policy.
- If the request is not matched with any forwarding policy, it is forwarded based on the default forwarding policy.

Forwarding Rule

Advanced forwarding policies support the following types of forwarding rules: domain name, path, HTTP request method, HTTP header, query string, cookie, and CIDR block.

Table 1-30 Forwarding rules

Forwarding Rule	Description
Domain name	<ul style="list-style-type: none"> ● Description Route requests based on the domain name. You can configure multiple domain names with each consist of at least two labels separated by periods (.). Max total: 100 characters. Max label: 63 characters. ● Matching rules <ul style="list-style-type: none"> – Exact match and wildcard match: The domain name can contain only letters, digits, and special characters <code>.-?=\~_+^\^*!\$& ()[]</code>. Asterisks (*) and question marks (?) can be used as wildcards. The domain name cannot start or end with a period (.) or contain two consecutive periods (..). – Regular expression match: The domain name can contain only letters, digits, and special characters <code>.-?=\~_+^\^*!\$& ()[]</code>. <p>Example Request URL: https://www.example.com/login.php?locale=en-us#videos Domain name in the forwarding rule: www.example.com</p>
Path	<ul style="list-style-type: none"> ● Description Route requests based on paths. You can configure multiple paths in a forwarding policy. Each path contains 1 to 128 characters, including letters, digits, and special characters: <code>_~!;@^-%#\$.*+?,=!: \/()[]{}</code> ● Matching rules <ul style="list-style-type: none"> – Exact match: The request path must exactly match that specified in the forwarding policy. The URL must start with a slash (/) and can use asterisks (*) and question marks (?) as wildcards. – Prefix match: The request path starts with the specified path string. The URL must start with a slash (/) and can use asterisks (*) and question marks (?) as wildcards. – Regular expression match: The URLs are matched using a regular expression. <p>For more information about path matching rules, see Path Matching.</p> <p>Example path: Request URL: https://www.example.com/login.php?locale=en-us#videos Path in the forwarding rule: /login.php</p>

Forwarding Rule	Description
Query string	<p>Route requests based on the query string.</p> <p>A query string consists of a key and one or more values. You need to set the key and values separately.</p> <ul style="list-style-type: none"> The key can contain only letters, digits, and special characters: !\$'()*+.,/;=?@^_-' Multiple values can be configured for a key. The value can contain letters, digits, and special characters: !\$'()*+.,/;=?@^_-' . Asterisks (*) and question marks (?) can be used as wildcard characters. <p>Example Request URL: https://www.example.com/login.php?locale=en-us#videos A query string needs to be configured for the forwarding rule: Key: locale Value: en-us</p>
HTTP request method	<p>Route requests based on the HTTP method.</p> <ul style="list-style-type: none"> You can configure multiple request methods in a forwarding policy. The following methods are available: GET, POST, PUT, DELETE, PATCH, HEAD, and OPTIONS. <p>Example GET</p>
HTTP header	<p>Route requests based on the HTTP header.</p> <p>An HTTP header consists of a key and one or more values. You need to configure the key and values separately.</p> <ul style="list-style-type: none"> The key can contain only letters, digits, underscores (_), and hyphens (-). <p>NOTE The first letter of HTTP request headers User-agent and Connection must be capitalized.</p> <ul style="list-style-type: none"> Multiple values can be configured for a key. The value can contain letters, digits, and special characters: !#\$%&'()*+.,\/:;<=>?@[^_-'{}~. Asterisks (*) and question marks (?) can be used as wildcard characters. <p>Example Key: Accept-Language Value: en-us</p>
CIDR block	<p>Route requests based on the source IP addresses from where requests originate.</p> <p>Example 192.168.1.0/24 or 2020:50::44/127</p>

Forwarding Rule	Description
Cookie	<p>Route requests based on the cookie.</p> <p>A cookie consists of a key and a value. You need to configure the key and value separately.</p> <ul style="list-style-type: none"> • A key can contain 1 to 100 characters and cannot start or end with a space. • A key can have one value, which can contain 1 to 100 characters. <p>You can enter multiple key-value pairs. The key-value pairs can contain letters, digits, and special characters <code>!%'"()*+.,/:=?@^_`~</code></p> <p>Example: Key: cookie_name Value: cookie_value</p>

Action Types

Advanced forwarding policies support the following actions: forward to a backend server group, redirect to another listener, redirect to another URL, and return a specific response body.

If you set **Action** to **Forward to backend server group** or **Return a specific response body**, you can add additional actions. ELB first performs additional actions and then forwards requests to the specified backend server group or returns a specific response body. Among all the additional actions, **Limit request** has the highest priority.

The following additional actions are supported:

- Forward to backend server group: rewrite, write header, remove header, and limit request
- Return a specific response body: limit request.

Table 1-31 Actions of an advanced forwarding policy

Action	Description
Forward to a backend server group	<p>Requests are forwarded to the specified backend server group.</p> <p>NOTE If Action is set to Forward to a backend server group, you can also select from one of the following additional actions: rewrite, write header, remove header, and limit request. For details, see Table 1-32.</p>

Action	Description
Redirect to another listener	<p>Requests are redirected to another listener, which then routes the requests to its associated backend server group.</p> <p>NOTE</p> <p>If you select Redirect to another listener, the configurations for the HTTP listener will not be applied, but access control configured for the listener will still be applied.</p> <p>For example, if you configure a redirect for an HTTP listener, HTTP requests to access a web page will be redirected to the HTTPS listener you select and handled by the backend servers associated with the HTTPS listener. As a result, the clients access the web page over HTTPS.</p>
Redirect to another URL	<p>Requests are redirected to the configured URL.</p> <p>When clients access website A, the load balancer returns 302 or any other 3xx status code and automatically redirects the clients to website B. You can customize the redirection URL that will be returned to the clients.</p> <p>Configure at least one of the following components:</p> <ul style="list-style-type: none">• Protocol: <code>#{protocol}</code>, HTTP, or HTTPS <code>#{protocol}</code>: retains the protocol of the request.• Domain Name: A domain name consists of at least two labels separated by periods (.). Each label can contain only letters, digits, hyphens (-), and periods (.), must start with a letter, digit, or asterisk (*), and cannot end with a hyphen (-). <code>#{host}</code>: retains the domain name of the request.• Port: ranges from 1 to 65535. <code>#{port}</code>: retains the port number of the request.• Path: A path can contain letters, digits, and special characters: <code>_~!;@^-%#&\$.*+?=: \/()[]{}</code> and must start with a slash (/). <code>#{path}</code>: retains the path of the request. <p>NOTE</p> <p>If you select regular expression match, the request path will be overwritten by the variables that match the regular expressions. For details, see Path Matching Based on Regular Expressions.</p> <ul style="list-style-type: none">• Query String: A query string can contain only letters, digits, and special characters: <code>!\$'()*+.,/:;=?@&^_-'&</code>. Ampersands (&) can only be used as separators.• HTTP Status Code: 301, 302, 303, 307, or 308 <p>Example</p> <p>URL for redirection: <code>http://www.example1.com/index.html?locale=en-us#videos</code></p> <p>Protocol: HTTP</p> <p>Domain name: <code>www.example1.com</code></p> <p>Port: 8081</p> <p>Path: <code>/index.html</code></p> <p>Query String: <code>locale=en-us</code></p> <p>HTTP Status Code: 301</p>

Action	Description
Return a specific response body	<p>Load balancers return a fixed response to the clients. You can custom the status code and response body that load balancers directly return to the clients without the need to route the requests to backend servers.</p> <p>Configure the following components:</p> <ul style="list-style-type: none">● HTTP Status Code: By default, 2xx, 4xx, and 5xx status codes are supported.● Content-Type: text/plain, text/css, text/html, application/javascript, or application/json● Message Body: This parameter is optional. The value is a string of 0 to 1,024 characters. <p>NOTE If Action is set to Return a specific response body, you can also select the additional action Limit request. For details, see Table 1-32.</p> <p>Example</p> <p>text/plain Sorry, the language is not supported.</p> <p>text/css <head><style type="text/css">div {background-color:red}#div {font-size:15px;color:red}</style></head></p> <p>text/html <form action="/" method="post" enctype="multipart/form-data"><input type="text" name="description" value="some text"><input type="file" name="myFile"><button type="submit">Submit</button></form></p> <p>NOTE To display languages other than English, you are advised to add <meta charset="utf-8"> to the message body. If you do not do this, the languages may appear as garbled characters.</p> <p>application/javascript String.prototype.trim = function() {var reExtraSpace = /\s*(.*?)\s\$/;return this.replace(reExtraSpace, "\$1")}</p> <p>application/json { "publicip": { "type": "5_bgp", "ip_version": 4}, "bandwidth": { "name": "bandwidth123", "size": 10, "share_type": "PER"}}</p> <p>NOTE Ensure that the response body does not contain carriage return characters. Otherwise, it cannot be saved.</p>

Table 1-32 Actions (optional)

Action	Description
Rewrite	<p>Rewrites the request URL before forwarding requests to the specified backend server group.</p> <p>Configure the following parameters:</p> <ul style="list-style-type: none">● Domain Name: A domain name consists of at least two labels separated by periods (.). Each label can contain only letters, digits, hyphens (-), and periods (.), must start with a letter, digit, or asterisk (*), and cannot end with a hyphen (-). `\${host}`: retains the domain name of the request.● Path: A path can contain letters, digits, and special characters: <code>_~!;@^-%#&\$.*+?,=!: \/()[]{}</code> and must start with a slash (/). `\${path}`: retains the path of the request. <p>NOTE</p> <p>If you select regular expression match, the request path will be overwritten by the variables that match the regular expressions. For details, see Path Matching Based on Regular Expressions.</p> <ul style="list-style-type: none">● Query String: A query string can contain only letters, digits, and the following special characters: <code>!\$'()*+.,/:;=?@&^_-'</code>, and ampersand (&) can only be used as a separator. <p>NOTE</p> <p>The domain name, path, and query string cannot be left blank or made default.</p>

Action	Description
Write header	<p>Writes the configured header into the request before forwarding it to the specified backend server group.</p> <p>You can specify the key and value of the header you want to write into the request that matches the forwarding rule. The headers you have configured will overwrite the existing headers. By default, you can configure five headers.</p> <p>A header consists of a key and one or more values. You need to configure the key and values separately.</p> <ul style="list-style-type: none">• Key: A key contains 1 to 40 characters and can contain only letters, digits, underscores (_), and hyphens (-).• A key can have one or more values. The value contains 1 to 128 characters, including only letters, digits, and special characters: !#\$%&'()*+,-./:;<=>@[^_`{ }~. Asterisks (*) and question marks (?) can be used as wildcard characters.<ul style="list-style-type: none">- Manually-defined value: Manually specify a header value. Each value cannot start or end with a space and can contain only letters, digits, and special characters: !#\$%&'()*+,-./:;<=>@[^_`{ }~- System-defined value: The following options are supported. Client port, client IP address, request protocol, load balancer instance ID, listener port, load balancer EIP, and load balancer private IP- Reference value: Use the value of a request header. The value can contain only letters, digits, underscores (_), and hyphens (-). <p>For details about how to write a header, see Table 1-33.</p>
Remove header	<p>Removes the configured headers from the request before forwarding it to the specified backend server group.</p> <p>You can specify the value of the header you want to remove from the request that matches the forwarding rule. The headers match the ones you have configured will be removed from the requests. By default, you can configure five headers.</p> <p>The key can contain only letters, digits, underscores (_), and hyphens (-).</p>

Action	Description
Limit request	<p>Limits the maximum number of queries per second if Forward to a backend server group or Return a specific response body is selected as the action.</p> <p>You need to configure the following parameters:</p> <ul style="list-style-type: none"> • QPS (Total): Specifies the maximum number of queries per second (QPS). The value ranges from 1 to 100000. If the number of requests reaches the specified value, new requests will be discarded and 503 Service Unavailable will be returned to the client. • QPS (Client IP Address): Specifies the maximum number of QPS from a source IP address. The value ranges from 1 to 100000. If both QPS (Total) and QPS (Client IP Address) are configured, the latter value must be smaller than the former. If the number of requests reaches the specified value, new requests will be discarded and 503 Service Unavailable will be returned to the client. <p>NOTE QPS (Client IP Address) is not available for QUIC listeners.</p>

Table 1-33 Writing a header

Request Header	Header Key	Header Value		Written Request Header
header1:aaa header2:bbb	header3	Manually defined value	ccc	header1:aaa header2:bbb header3:ccc
	header3	System-defined value	Client port	header1:aaa header2:bbb header3: <i>Client port</i>
	header3	Reference value	header1	header1:aaa header2:bbb header3:aaa

 **NOTE**

The value of the following headers (case-insensitive) cannot be modified:

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, and x-nuwa-trace-ne-out.

Path Matching

Table 1-34 shows how paths configured in the forwarding policies match those in the requests.

Table 1-34 Path matching examples

Request Path	Forwarding Policy	Specified Path	Matching Mode	Forwarding Policy Priority	Destination Backend Server Group
/elb/ abc.html	Forwarding policy 01	/elb/abc.html	Prefix match	1	Backend server group 01
	Forwarding policy 02	/elb	Prefix match	2	Backend server group 02
/exa/ index.html	Forwarding policy 03	/exa[^\s]*	Regular expression match	3	Backend server group 03
	Forwarding policy 04	/exa/ index.html	Regular expression match	4	Backend server group 04
/mpl/ index.html	Forwarding policy 05	/mpl/ index.html	Exact match	5	Backend server group 05

URLs are matched as follows:

- When the request path is /elb/abc.html, it matches both forwarding policy 01 and forwarding policy 02. However, the priority of forwarding policy 01 is higher than that of forwarding policy 02. Forwarding policy 01 is used, and requests are forwarded to backend server group 01.
- When the request path is /exa/index.html, it matches both forwarding policy 03 and forwarding policy 04. However, the priority of forwarding policy 03 is higher than that of forwarding policy 04. Forwarding policy 03 is used, and requests are forwarded to backend server group 03.
- If the request path is /mpl/index.html, it matches forwarding policy 05 exactly, and requests are forwarded to backend server group 05.

Path Matching Based on Regular Expressions

A path can contain letters, digits, and special characters: `_~!;@^-%#&$.*+?,=!:|\/()[]{}` and must start with a slash (`/`). `#{path}` retains the path of the request.

If you select regular expression match, the request path will be overwritten by the variables that match the regular expressions.

How Request Paths Are Overwritten

1. Path matching: The client sends a request, and the request matches a regular expression in the forwarding rule. You can specify one or more regular expressions as the match conditions and set multiple capture groups represented by parentheses (`)` for one regular expression.
2. Extraction and replacement: extracts the content from the capture groups.
3. Destination path: writes them to `$1`, `$2`, all the way to `$9` configured for the path.

Example

When a client requests to access `/test/ELB/elb/index`, which matches the regular expression `/test/(.*/)(.*/)index`, `$1` will be replaced by `ELB` and `$2` by `elb`, and then the request will be redirected to `/ELB/elb`.

Table 1-35 URL matching based on regular expressions

Matching Step		Description
Forwarding rule: path	Regular expression match	<ul style="list-style-type: none">• Matching condition: <code>/test/(.*/)(.*/)index</code>• Request path: <code>/test/ELB/elb/index</code>
Action: rewrite or redirect to another URL	Path	<ul style="list-style-type: none">• Path: <code>/\$1/\$2</code>• Extracting content <code>\$1: ELB</code> <code>\$2: elb</code>• Destination path: <code>/ELB/elb</code>

1.4.3.5.2 Managing an Advanced Forwarding Policy

Scenarios

You can configure advanced forwarding policies for HTTP or HTTPS listeners of dedicated load balancers to route requests more specifically.

Each advanced forwarding policy consists of one or more forwarding rules and an action.

- Dedicated load balancers support the following types of forwarding rules: domain name, path, HTTP request method, HTTP header, query string, cookie, and CIDR block. For details, see [Forwarding Rule](#).
- Advanced forwarding policies support the following actions: forward to a backend server group, redirect to another listener, redirect to another URL,

rewrite, write header, remove header, limit request, and return a specific response body. For details, see [Action Types](#).

- Multiple forwarding rules can be configured in a single forwarding policy.
- Forwarding policies can be sorted based on their priorities.

Notes and Constraints

- Advanced forwarding cannot be disabled once enabled.
- An advanced forwarding policy can contain a maximum of 10 conditions.

Enabling Advanced Forwarding

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer you want to configure forwarding policies for and click its name.
3. Click the **Listeners** tab and click the target listener.
4. On the **Summary** tab, click **Enable** next to **Advanced Forwarding**.
5. Click **OK**.

Adding an Advanced Forwarding Policy

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer you want to configure forwarding policies for and click its name.
3. On the **Listeners** tab, add a forwarding policy in either of the following ways:
 - Locate the target listener and click **Add/Edit Forwarding Policy** in the **Forwarding Policies** column.
 - Locate the target listener, click its name, and click the **Forwarding Policies** tab.
4. Click **Add Forwarding Policy** and configure the parameters based on [Table 1-30](#) and [Table 1-31](#).
5. Click **Save**.

Sorting Forwarding Policies

Each listener can have multiple forwarding policies, which are matched in descending order of priority. A smaller value indicates a higher priority.

You can adjust the priority of custom forwarding policies, but the priority of the default forwarding policy cannot be changed.

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer whose forwarding policies you want to modify and click its name.
3. Click **Listeners**, locate the listener, and click its name.
4. On the **Forwarding Policies** tab, click **Sort**.
5. Drag the forwarding policies to adjust their priorities.
6. Click **Save**.

Modifying a Forwarding Policy

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer whose forwarding policies you want to modify and click its name.
3. Click **Listeners**, locate the listener, and click its name.
4. On the **Forwarding Policies** tab, select the forwarding policy, and click **Edit**.
5. Modify the parameters and click **Save**.

Deleting a Forwarding Policy

You can delete a forwarding policy if you no longer need it.

Deleted forwarding policies cannot be recovered.

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer whose forwarding policies you want to delete and click its name.
3. Click **Listeners**, locate the listener, and click its name.
4. On the **Forwarding Policies** tab, select the forwarding policy and click **Delete** on the top right.
5. In the displayed dialog box, click **OK**.

1.4.3.6 HTTP Headers

HTTP headers are a list of strings sent and received by both the client and server on every Hypertext Transfer Protocol (HTTP) request and response. This section describes HTTP headers supported by HTTP and HTTP listeners.

Table 1-36 Transfer headers

Header	Feature	Description	Dedicated Load Balancers
X-Forwarded-ELB-IP	Transfer Load Balancer EIP	If this option is enabled, the EIP bound to the load balancer will be transmitted to backend servers through the X-Forwarded-ELB-IP header. The format is as follows (XX.XXX.XX.XXX indicates the EIP of the load balancer): X-Forwarded-ELB-IP: XX.XXX.XX.XXX	Supported
X-Forwarded-ELB-ID	Transfer Load Balancer ID	If this option is enabled, the load balancer ID will be transmitted to backend servers through the X-Forwarded-ELB-ID header.	Supported

Header	Feature	Description	Dedicated Load Balancers
X-Forwarded-Port	Transfer Listener Port Number	If this option is enabled, the port number used by the listener will be transmitted to backend servers through the X-Forwarded-Port header.	Supported
X-Forwarded-For-Port	Transfer Port Number in the Request	If this option is enabled, the port number used by the client will be transmitted to backend servers through the X-Forwarded-For-Port header.	Supported

Table 1-37 Rewrite headers

Header	Feature	Description	Dedicated Load Balancers
X-Forwarded-Host	Rewrite X-Forwarded-Host	<ul style="list-style-type: none">• If this option is enabled, the Host header of the client request will be rewritten into the X-Forwarded-Host header and transmitted to the backend servers.• If this option is disabled, the X-Forwarded-Host header of the client will be transmitted to the backend servers.	Supported
X-Forwarded-Proto	Rewrite X-Forwarded-Proto	<ul style="list-style-type: none">• If this option is enabled, the listener protocol will be rewritten into the X-Forwarded-Proto header field and transmitted to the backend servers.• If this option is disabled, the protocol used by the client will be transmitted to the backend servers through the X-Forwarded-Proto header.	Supported
X-Real-IP	Rewrite X-Real-IP	<ul style="list-style-type: none">• If this option is enabled, the source IP address of the client will be rewritten into the X-Real-IP header and transmitted to the backend servers.• If this option is disabled, the X-Real-IP header of the client will be transmitted to the backend servers.	Supported

 **NOTE**

- More HTTP headers are coming soon. See the available HTTP headers on the management console.
- ✓ indicates the load balancer supports the header, whereas × indicates the load balancer does not support the header.

Enabling HTTP/HTTPS Headers

1. Go to the [load balancer list page](#).
2. You can enable these header features in either of the following ways:
 - On the displayed page, locate the load balancer and click its name. Under **Listeners**, click **Add Listener**.
 - On the displayed page, locate the load balancer and click **Add Listener** in the **Operation** column.
3. On the **Configure Listener** page, expand **Advanced Settings** and enable the features as needed.
4. Configure the listener as prompted.
5. Confirm the configuration and click **Submit**.

Modifying HTTP Header Features

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
3. Click the **Listeners** tab, locate the target listener and click **Edit** in **Operation** column.
4. On the displayed page, expand **Advanced Settings** and enable or disable the features.
5. Click **OK**.

1.4.3.7 HTTP/2

What Is HTTP/2?

Hypertext Transfer Protocol 2.0 (HTTP/2) uses a binary format for data transmission. It allows for much faster transmission and multiplexing. To reduce latency and improve efficiency, you can enable HTTP/2 when you add HTTPS listeners.

Notes and Constraints

You can enable HTTP/2 only for HTTPS listeners.

Managing HTTP/2

You can enable HTTP/2 when you add an HTTPS listener. You can enable or disable HTTP/2 for an existing HTTPS listener.

Enabling HTTP/2 When Adding a Listener

To enable HTTP/2 when adding an HTTPS listener, perform the following operations:

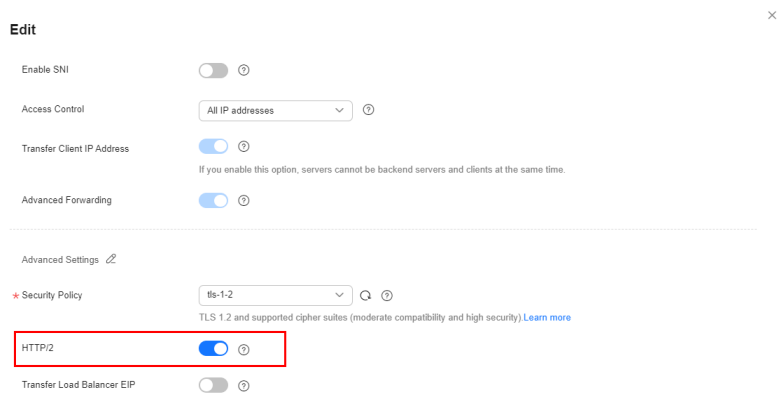
1. Go to the [load balancer list page](#).
2. Locate the load balancer and click its name.
3. Under **Listeners**, click **Add Listener**.
4. In the **Add Listener** dialog box, set **Frontend Protocol** to **HTTPS**.
5. Expand **Advanced Settings** and enable HTTP/2.
6. Confirm the configurations and go to the next step.

Figure 1-9 Enabling HTTP/2

The screenshot shows the 'Add Listener' configuration dialog box. The 'Frontend Protocol' is set to 'HTTPS'. In the 'Advanced Settings' section, the 'HTTP/2' toggle switch is turned on and highlighted with a red box. Other settings include: Name: listener-3265; Frontend Port: 443; SSL Authentication: One-way authentication; Server Certificate: [dropdown]; Access Control: All IP addresses; Transfer Client IP Address: [checked]; Security Policy: ts-1-2; Transfer Load Balancer EIP: [unchecked].

Enabling or Disabling HTTP/2 for an Existing Listener

1. Go to the [load balancer list page](#).
2. Locate the load balancer and click its name.
3. Click **Listeners**, locate the listener, and click its name.
4. On the **Summary** tab, click **Edit** on the top right.
5. In the **Edit** dialog box, expand **Advanced Settings** and enable or disable HTTP/2.
6. Click **OK**.

Figure 1-10 Disabling or enabling HTTP/2

1.4.4 Modifying a Listener

Scenarios

You can configure modification protection for a listener, modify the settings of a listener, change the backend server group of a listener, and delete a listener.

Prerequisites

- You have created a load balancer by referring to [Creating a Dedicated Load Balancer](#).
- You have created a backend server group by referring to [Creating a Backend Server Group](#).
- You have added a listener by referring to [Listener Overview](#).

Configuring Modification Protection for a Listener

You can enable modification protection for a listener to prevent it from being modified or deleted by accident.

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
3. Click **Listeners** tab, locate the listener, and click its name.
4. On the **Summary** tab, click **Configure** next to **Modification Protection**.
5. In the **Configure Modification Protection** dialog box, enable **Modification Protection**.

NOTE

You need to disable **Modification Protection** if you want to modify or delete a listener.

Modifying Listener Settings

NOTE

Frontend Protocol/Port and **Backend Protocol** cannot be modified. If you want to modify the protocol or port of the listener, add another listener to the load balancer.

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
3. Modify the listener in either of the following ways:
 - On the **Listeners** tab, locate the listener, and click **Edit** in the **Operation** column.
 - Click the name of the target listener. On the **Summary** tab, click **Edit** on the top right corner.
4. In the **Edit** dialog box, modify parameters, and click **OK**.

Modifying Timeout Durations

You can modify timeout durations (idle timeout, request timeout, and response timeout) for your listeners to meet varied demands. For example, if the size of a request from an HTTP or HTTPS client is large, you can prolong the request timeout duration to ensure that the request can be successfully routed.

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
3. Click **Listeners**, locate the listener, and click the name of the listener.
4. On the **Summary** tab, click **Edit** on the top right.
5. In the **Edit** dialog box, expand **Advanced Settings**.
6. Configure **Idle Timeout (s)**, **Request Timeout (s)**, or **Response Timeout (s)** as you need.
7. Click **OK**.

Changing the Backend Server Group of a Listener

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the target load balancer and click its name.
3. On the **Listeners** tab, locate the target listener and click its name.
4. On the **Summary** tab, click **Change Backend Server Group** on the right of **Default Backend Server Group** area.
5. In the displayed dialog box, click the server group name box.
Select a backend server group from the drop-down list or create a group.
 - a. Click the name of the backend server group or enter the name in the search box to search for the target group.
 - b. Click **Create Backend Server Group**. After the backend server group is created, click the refresh icon.

NOTE

The backend protocol of the new backend server group must match the frontend protocol of the listener.

6. Click **OK**.

Deleting a Listener

1. Go to the [load balancer list page](#).

2. On the displayed page, locate the load balancer and click its name.
3. Click the **Listeners** tab, locate the listener, and click **Delete** in the **Operation** column.
4. In the displayed dialog box, enter **DELETE**.
5. Click **OK**.

1.5 Backend Server Group

1.5.1 Backend Server Group Overview

What Is a Backend Server Group?

A backend server group is a logical collection of one or more backend servers to receive massive concurrent requests at the same time. A backend server can be a cloud server, supplementary network interface, or IP address.

The following table describes how a backend server group forwards traffic.

Table 1-38 Traffic distribution process

Step 1	A client sends a request to your application. The listeners added to your load balancer use the protocols and ports you have configured to forward the request to the associated backend server group.
Step 2	Healthy backend servers in the backend server group receive the request based on the load balancing algorithm, handle the request, and return a result to the client.
Step 3	In this way, massive concurrent requests can be processed at the same time, improving the availability of your applications.

For dedicated load balancers, the backend server group type can be **Hybrid** or **IP as a backend server**. You can add cloud servers, supplementary network interfaces, or IP addresses to a hybrid backend server group. If you set the type to **IP as a backend server**, you can only add IP addresses as backend servers.

Figure 1-11 shows the architecture of different types of backend server groups.

Figure 1-11 Backend server group architecture

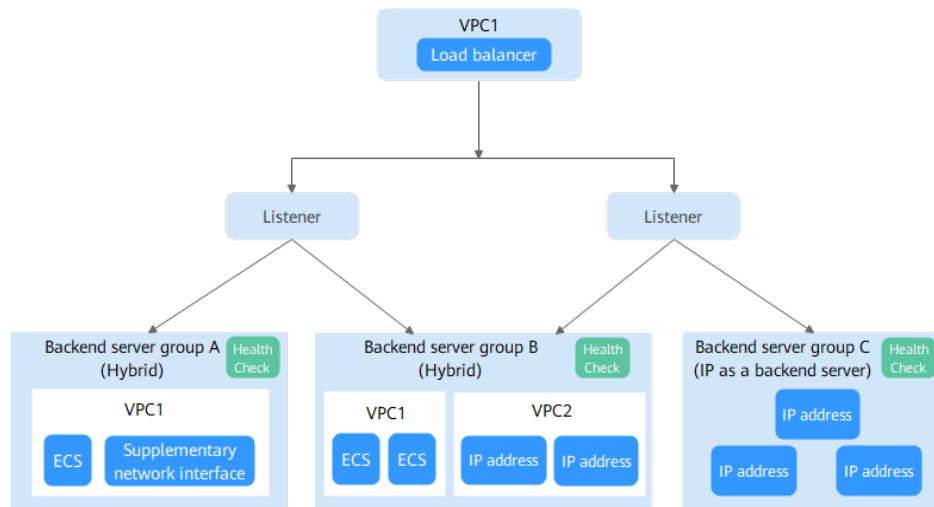


Table 1-39 Backend server group types

Backend Server Group Type	Backend Server Type	Example
Hybrid	<ul style="list-style-type: none"> Cloud servers and supplementary network interfaces that are in the same VPC as the load balancer Cloud servers in other VPCs or on-premises servers if IP as a backend is enabled for the load balancer 	<p>As shown in Figure 1-11:</p> <ul style="list-style-type: none"> In backend server group A, you can add ECSs or supplementary network interfaces in VPC1. In backend server group B, you can add IP addresses in VPC2 as backend servers.
IP as a backend server	IP addresses of cloud servers in other VPCs or on-premises servers if IP as a backend is enabled for the load balancer	As shown in Figure 1-11 , IP addresses can be added to backend server group C as backend servers.

Advantages

Backend server groups can bring the following benefits:

- Reduced costs and easier management:** You can add or remove backend servers as traffic changes over the time. This can help avoid low resource utilization and makes it easy to manage backend servers.
- Higher reliability:** Traffic is routed only to healthy backend servers in the backend server group.

Controlling Traffic Distribution

You can configure the key functions listed in [Table 1-40](#) for each backend server group to ensure service stability.

Table 1-40 Key functions

Key Function	Description	Detail
Forwarding Mode	<p>Specifies the forwarding mode used by the load balancer to distribute traffic.</p> <p>There are two options: Load balancing and Active/Standby.</p> <ul style="list-style-type: none">• Load balancing: Multiple backend servers can be added to this type of backend server group. The load balancer distributes requests across these backend servers based on the load balancing algorithm configured for this backend server group.• Active/Standby: Only two backend servers can be added to the backend server group, one acting as the active server and the other as the standby server. The load balancer routes the traffic to the active server if it works normally. If the active server becomes unhealthy, the load balancer then routes the traffic to the standby server.	Creating a Backend Server Group
Load Balancing Algorithm	<p>The load balancer distributes traffic based on the load balancing algorithm you have configured for the backend server group.</p>	Load Balancing Algorithms
Sticky Session	<p>Specifies whether to enable the sticky session option. If you enable this option, all requests from a client during one session are sent to the same backend server.</p>	Sticky Session
Slow Start	<p>Specifies whether to enable slow start. After you enable it, the load balancer linearly increases the proportion of requests to new backend servers in the backend server group.</p> <p>When the slow start duration elapses, the load balancer sends full share of requests to these backend servers and exits the slow start mode.</p>	Slow Start

Key Function	Description	Detail
Forward to Same Port	<p>Specifies whether to enable the forward to same port option. After you enable it, you do not need to specify a backend port when you add a backend server. The listener routes the requests to the backend server over the same port as the frontend port.</p> <p>NOTE This option is available only for TCP, UDP, or QUIC backend server groups associated with a dedicated load balancer.</p>	Creating a Backend Server Group

Backend Server Group and Listener Protocols

You can associate a backend server group with different dedicated load balancers under the same enterprise project or different listeners.

The backend protocol of the new backend server group must match the frontend protocol of the listener as described in [Table 1-41](#).

Table 1-41 The frontend and backend protocol

Load Balancer Specification	Frontend Protocol	Backend Protocol
Network load balancing	TCP	TCP
Network load balancing	UDP	<ul style="list-style-type: none">• UDP• QUIC
Network load balancing	TLS	<ul style="list-style-type: none">• TLS• TCP
Application load balancing	HTTP	HTTP
Application load balancing	HTTPS	<ul style="list-style-type: none">• HTTP• HTTPS• gRPC
Application load balancing	QUIC	<ul style="list-style-type: none">• HTTP• HTTPS• gRPC

 NOTE

TLS, gRPC, and QUIC will be available in more regions. You can see which regions support them on the console.

1.5.2 Creating a Backend Server Group

Scenario

To route requests, you need to associate at least one backend server group to each listener.

A backend server group can be associated with more than one listener.

You can create a backend server group for a load balancer in any of the ways described in [Table 1-42](#).

Table 1-42 Scenarios

Scenario	Reference
Creating a backend server group and associating it with a load balancer	Procedure
Creating a backend server group when adding a listener	You can add listeners using different protocols by referring to Listener Overview .
Changing the backend server group associated with the listener	Changing a Backend Server Group

Notes and Constraints

The backend protocol of the new backend server group must match the frontend protocol of the listener as described in [Table 1-43](#).

Table 1-43 The frontend and backend protocol

Load Balancer Specification	Frontend Protocol	Backend Protocol
Network load balancing	TCP	TCP
Network load balancing	UDP	<ul style="list-style-type: none">• UDP• QUIC
Network load balancing	TLS	<ul style="list-style-type: none">• TLS• TCP

Load Balancer Specification	Frontend Protocol	Backend Protocol
Application load balancing	HTTP	HTTP
Application load balancing	HTTPS	<ul style="list-style-type: none">• HTTP• HTTPS• gRPC
Application load balancing	QUIC	<ul style="list-style-type: none">• HTTP• HTTPS• gRPC

Procedure

1. Go to the [backend server group list page](#).
2. Click **Create Backend Server Group** in the upper right corner.
3. Configure the routing policy based on [Table 1-44](#).

Table 1-44 Parameters required for configuring a routing policy

Parameter	Description
Load Balancer Type	Specifies the type of load balancers that can use the backend server group. Select Dedicated .
Load Balancer	Specifies whether to associate a load balancer. You can associate an existing dedicated load balancer when you create a backend server group or associate one later. <ul style="list-style-type: none">• Associate later• Associate existing
Forwarding Mode	Specifies the forwarding mode to distribute traffic. There are two options: Load balancing and Active/Standby . <ul style="list-style-type: none">• Load balancing: You can add one or more backend servers to the backend server group.• Active/Standby: You must add two backend servers to the backend server group, one acting as the active server and the other as the standby server. If the active server is faulty, traffic is forwarded to the standby server, improving service reliability. Active/standby backend server groups can only be associated with TCP, UDP, and TLS listeners.

Parameter	Description
Backend Server Group Type	<p>Specifies the type of the backend server group.</p> <ul style="list-style-type: none">● Hybrid: You can add ECSs and supplementary network interfaces as backend servers, or add IP addresses as servers when IP as a Backend is enabled. When you create a hybrid backend server group, you must specify a VPC and associate the backend server group with a load balancer in this VPC.● IP as a backend server: You can add IP addresses as backend servers only when you enable IP as a Backend. <p>NOTE This option is available in certain regions. You can see which regions support this option on the console.</p>
Backend Server Group Name	<p>Specifies the name of the backend server group.</p>
VPC	<p>Specifies the VPC where the backend server group works. You can associate the backend server group with a load balancer in this VPC.</p> <p>This parameter is mandatory if you select Hybrid for Backend Server Group Type.</p> <p>You can select an existing VPC or create a new one. For more information about VPC, see the Virtual Private Cloud User Guide.</p>
Backend Protocol	<p>Specifies the protocol that backend servers in the backend server group use to receive requests from the listeners. The protocol varies depending on the forwarding mode:</p> <ul style="list-style-type: none">● Load balancing: HTTP, HTTPS, gRPC, TCP, UDP, TLS, or QUIC● Active/Standby: TCP, UDP, TLS, or QUIC
IP Address Type	<p>Specifies the IP address type of backend servers that can be added to a backend server group. By default, IPv4 addresses can be added as backend servers.</p> <p>There are two options when the backend protocol is TCP or UDP:</p> <ul style="list-style-type: none">● IPv4: Only IPv4 addresses can be added as backend servers.● Dual stack: Both IPv4 and IPv6 addresses can be added as backend servers. <p>NOTE This option is available in certain regions. You can see which regions support this option on the console.</p>

Parameter	Description
Forward to Same Port	<p>If this option is enabled, you do not need to specify a backend port when you add a backend server. The listener routes the requests to the backend server over the same port as the frontend port.</p> <p>This option cannot be disabled after being enabled.</p> <p>NOTE This option is available in certain regions. You can see which regions support this option on the console.</p> <p>NOTE This option is available only for TCP, UDP, or QUIC backend server groups associated with a dedicated load balancer.</p>
Load Balancing Algorithm	<p>Specifies the algorithm used by the load balancer to distribute traffic. The following options are available:</p> <ul style="list-style-type: none">• Weighted round robin: Requests are routed to different servers based on their weights. Backend servers with higher weights receive proportionately more requests, whereas equal-weighted servers receive the same number of requests.• Weighted least connections: In addition to the number of connections, each server is assigned a weight based on its capacity. Requests are routed to the server with the lowest connections-to-weight ratio.• Source IP hash: Allows requests from different clients to be routed based on source IP addresses and ensures that requests from the same client are forwarded to the same server.• Connection ID: This algorithm is available when you have selected QUIC for Backend Protocol. This algorithm allows requests with different connection IDs to be routed to different backend servers and ensures that requests with the same connection ID are routed to the same backend server. <p>For more information about load balancing algorithms, see Load Balancing Algorithms.</p>

Parameter	Description
Forwarding Even Unhealthy	<p>Specifies whether to forward traffic across all the backend servers even if all of them have been identified as unhealthy. This option is only available if Forwarding Mode is set to Load balancing.</p> <p>This option is disabled by default, preventing requests from being sent to the backend server group, in which all backend servers are identified as unhealthy.</p> <p>If this option is enabled, ELB forwards traffic across all the backend servers even if all of them have been identified as unhealthy.</p> <p>The function improves service availability by preventing disruptions from faulty health checks resulting from misconfigurations.</p>
Sticky Session	<p>Specifies whether to enable sticky sessions if you have selected Weighted round robin, Connection ID, or Weighted least connections for Load Balancing Algorithm.</p> <p>If you enable sticky sessions, all requests from the same client during one session are sent to the same backend server.</p> <p>For more information about sticky sessions, see Sticky Session.</p> <p>NOTE TLS backend server groups do not support sticky sessions.</p>
Sticky Session Type	<p>Specifies the sticky session type.</p> <p>This parameter is mandatory if Sticky Session is enabled. You can select one of the following types:</p> <ul style="list-style-type: none">● Source IP address: The source IP address of each request is calculated using the consistent hashing algorithm to obtain a unique hashing key, and all backend servers are numbered. The system allocates the client to a particular server based on the generated key. This allows requests from the same IP address are forwarded to the same backend server.● Load balancer cookie: The load balancer generates a cookie after receiving a request from the client. All subsequent requests with the cookie are routed to the same backend server. <p>NOTE</p> <ul style="list-style-type: none">● Source IP address is available when you have selected TCP, QUIC, or UDP for Backend Protocol.● Load balancer cookie and Application cookie are available when you have selected HTTP, GRPC, or HTTPS for Backend Protocol.


Parameter	Description
Stickiness Duration (min)	<p>Specifies the minutes that sticky sessions are maintained. This parameter is mandatory if Sticky Session is enabled.</p> <ul style="list-style-type: none">• Sticky sessions at Layer 4: 1 to 60• Sticky sessions at Layer 7: 1 to 1440
Slow Start	<p>Specifies whether to enable slow start. This parameter is optional if you have selected Weighted round robin for Load Balancing Algorithm.</p> <p>After you enable this option, the load balancer linearly increases the proportion of requests to backend servers in this mode.</p> <p>When the slow start duration elapses, the load balancer sends full share of requests to backend servers and exits the slow start mode.</p> <p>NOTE Slow start is only available for HTTP, gRPC, and HTTPS backend server groups of dedicated load balancers.</p> <p>For more information about the slow start, see Slow Start.</p>
Slow Start Duration (s)	<p>Specifies how long the slow start will last, in seconds.</p> <p>This parameter is mandatory if Slow Start is enabled.</p>
Deregistration Delay	<p>This parameter is enabled by default if the backend protocol is TCP, UDP, or QUIC.</p> <p>If a backend server is removed or the health check fails, ELB continues to route in-flight requests to this server until the deregistration delay timeout expires.</p> <p>NOTE This option is available in certain regions. You can see which regions support this option on the console.</p>
Deregistration Delay Timeout (s)	<p>This parameter is mandatory if Deregistration Delay is enabled.</p> <p>ELB continues to route in-flight requests to the backend server until the deregistration delay timeout expires.</p> <p>The value ranges from 10 to 4000, in seconds. The default value is 300.</p>
Description	<p>Provides supplementary information about the backend server group.</p>

4. Click **Next** to add backend servers and configure health check.

Add cloud servers, supplementary network interfaces, or IP addresses to this backend server group. For details, see [Backend Server Overview](#).

Configure health check for the backend server group based on [Table 1-45](#). For more information about health checks, see [Health Check](#).

Table 1-45 Parameters required for configuring a health check

Parameter	Description
Health Check	<p>Specifies whether to enable health checks.</p> <p>If the health check is enabled, click  next to Advanced Settings to set health check parameters.</p>
Health Check Protocol	<p>Specifies the protocol that will be used by the load balancer to check the health of backend servers.</p> <ul style="list-style-type: none">• TCP, HTTP, TLS, gRPC, and HTTPS are supported.• If the protocol of the backend server group is UDP and QUIC, the health check protocol is UDP by default and cannot be changed. <p>NOTE TLS and gRPC are available in certain regions. You can see which regions support them on the console.</p>
Domain Name	<p>Specifies the domain name that will be used for health checks.</p> <p>This parameter is mandatory if the health check protocol is HTTP, gRPC, or HTTPS.</p> <ul style="list-style-type: none">• By default, the private IP address of each backend server is used.• You can also specify a domain name that consists of at least two labels separated by periods (.). Use only letters, digits, and hyphens (-). Do not start or end strings with a hyphen. Max total: 100 characters. Max label: 63 characters.
Health Check Port	<p>Specifies the port that will be used by the load balancer to check the health of backend servers. The port number ranges from 1 to 65535.</p> <p>NOTE By default, the service port on each backend server is used. You can also specify a port for health checks.</p>

Parameter	Description
Path	<p>Specifies the health check URL, which is the destination on backend servers for health checks. This parameter is mandatory if the health check protocol is HTTP, gRPC, or HTTPS.</p> <p>The path can contain 1 to 80 characters and must start with a slash (/).</p> <p>The path can contain letters, digits, hyphens (-), slashes (/), periods (.), question marks (?), number signs (#), percent signs (%), ampersands (&), and extended character sets _~!. () *[]@\$^!'+</p>
Interval (s)	<p>Specifies the maximum time between two consecutive health checks, in seconds.</p> <p>The interval ranges from 1 to 50.</p>
Timeout (s)	<p>Specifies the maximum time required for waiting for a response from the health check, in seconds. The value ranges from 1 to 50.</p>
Healthy Threshold	<p>Specifies the number of consecutive successful health checks required for declaring a backend server healthy. The value ranges from 1 to 10.</p>
Unhealthy Threshold	<p>Specifies the number of consecutive failed health checks required for declaring a backend server unhealthy. The value ranges from 1 to 10.</p>
Status Code	<p>Specifies the status codes that will be returned to the load balancer to indicate the health of backend servers. This parameter is available only when you set the health check protocol to HTTP or HTTPS.</p> <p>You can enter a unique number or a positive number range within the status code range, for example, 0-10 and 200-300. A maximum of five HTTP status codes are supported. If there is more than one status code, press Enter to separate them.</p> <ul style="list-style-type: none">• If the health check protocol is HTTP or HTTPS, the status code ranges from 200 to 599.• When the gRPC protocol is used, the status code ranges from 0 to 99. <p>NOTE This feature will be available in more regions. See details on the management console.</p>

5. Click **Next**.
6. Confirm the specifications and click **Create Now**.

Related Operations

You can associate the backend server group with the listener of a dedicated load balancer in either way listed in [Table 1-42](#).

1.5.3 Controlling Traffic Distribution

1.5.3.1 Load Balancing Algorithms

Overview

Load balancers receive requests from clients and forward them to backend servers in one or more AZs. Each load balancer has at least a listener and a backend server. The load balancing algorithm you select when you create the backend server group determines how requests are distributed.

ELB supports the following load balancing algorithms: weighted round robin, weighted least connections, source IP hash, and connection ID.

The default load balancing algorithm is weighted round robin. You can change it to a different algorithm if needed.

You can select the load balancing algorithm that best suits your needs.

Table 1-46 Load balancing algorithms

Load Balancing Algorithm	Description
Weighted round robin	Routes requests to backend servers in sequence based on their weights.
Weighted least connections	Routes requests to backend servers with the smallest connections-to-weight ratio.
Consistent hashing <ul style="list-style-type: none">Source IP hashConnection ID	Calculates the request fields using the consistent hashing algorithm to obtain a hash value and routes requests with the same hash value to the same backend server, even if the number of backend servers in the backend server group changes. <ul style="list-style-type: none">Source IP hash: Calculates the source IP address of each request and routes requests from the same source IP address to the same backend server.Connection ID: Calculates the QUIC connection ID and routes requests with the same ID to the same backend server.

How Load Balancing Algorithms Work

Dedicated load balancers support four load balancing algorithms: weighted round robin, weighted least connections, source IP hash, and connection ID.

Weighted Round Robin

Figure 1-12 shows an example of how requests are distributed using the weighted round robin algorithm. Two backend servers are in the same AZ and have the same weight, and each server receives the same proportion of requests.

Figure 1-12 Traffic distribution using the weighted round robin algorithm

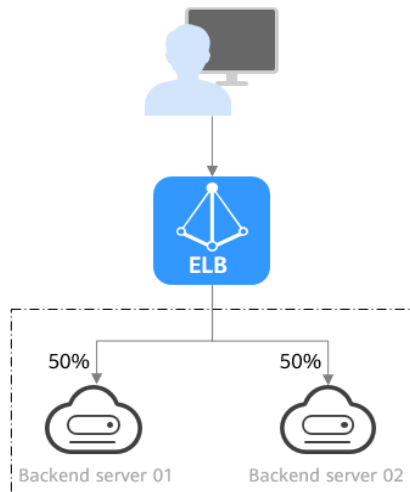


Table 1-47 Weighted round robin

Description	Requests are routed to backend servers in sequence based on their weights. Backend servers with higher weights receive proportionately more requests, whereas equal-weighted servers receive the same number of requests.
When to Use	<p>This algorithm is typically used for short connections, such as HTTP connections.</p> <ul style="list-style-type: none"> Flexible load balancing: When you need more refined load balancing, you can set a weight for each backend server to specify the percentage of requests to each server. For example, you can set higher weights to backend servers with better performance so that they can process more requests. Dynamic load balancing: You can adjust the weight of each backend server in real time when the server performance or load fluctuates.
Disadvantages	<ul style="list-style-type: none"> You need to set a weight for each backend server. If you have a large number of backend servers or your services require frequent adjustments, setting weights would be time-consuming. If the weights are inappropriate, the requests processed by each server may be imbalanced. As a result, you may need to frequently adjust server weights.

Weighted Least Connections

Figure 1-13 shows an example of how requests are distributed using the weighted least connections algorithm. Two backend servers are in the same AZ and have the same weight, 100 connections have been established with backend server 01, and 50 connections have been established with backend server 02. New requests are preferentially routed to backend server 02.

Figure 1-13 Traffic distribution using the weighted least connections algorithm

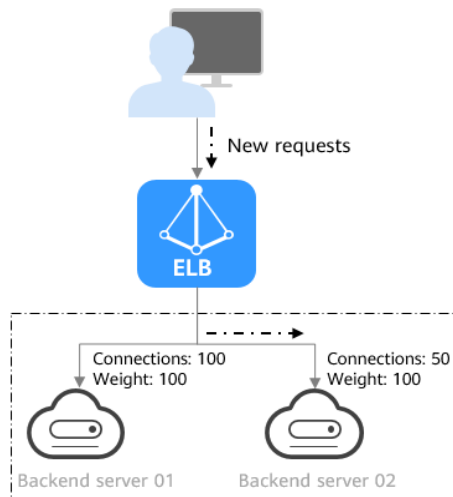


Table 1-48 Weighted least connections

Description	In addition to the number of active connections established with each backend server, each server is assigned a weight based on their processing capability. Requests are routed to the server with the lowest connections-to-weight ratio.
When to Use	<p>This algorithm is often used for persistent connections, such as connections to a database.</p> <ul style="list-style-type: none"> • Flexible load balancing: Load balancers distribute requests based on the number of established connections and the weight of each backend server and route requests to the server with the lowest connections-to-weight ratio. This helps prevent servers from being underloaded or overloaded. • Dynamic load balancing: When the number of connections to and loads on backend servers change, you can use the weighted least connection algorithm to dynamically adjust the requests distributed to each server in real time. • Stable load balancing: You can use this algorithm to reduce the peak loads on each backend server and improve service stability and reliability.

Disadvantages	<ul style="list-style-type: none"> • Complex calculation: The weighted least connections algorithm needs to calculate and compare the number of connections established with each backend server in real time before selecting a server to route requests. • Dependency on connections to backend servers: The algorithm routes requests based on the number of connections established with each backend server. If monitoring data is inaccurate or outdated, requests may not be distributed evenly across backend servers. The algorithm can only collect statistics on the connections between a given load balancer and a backend server, but cannot obtain the total number of connections to the backend server if it is associated with multiple load balancers. • Too many loads on new servers: If existing backend servers have to handle a large number of requests, new requests will be routed to new backend servers. This may deteriorate new servers or even cause them to fail.
----------------------	--

Source IP Hash

Figure 1-14 shows an example of how requests are distributed using the source IP hash algorithm. Two backend servers are in the same AZ and have the same weight. If backend server 01 has processed a request from IP address A, the load balancer will route new requests from IP address A to backend server 01.

Figure 1-14 Traffic distribution using the source IP hash algorithm

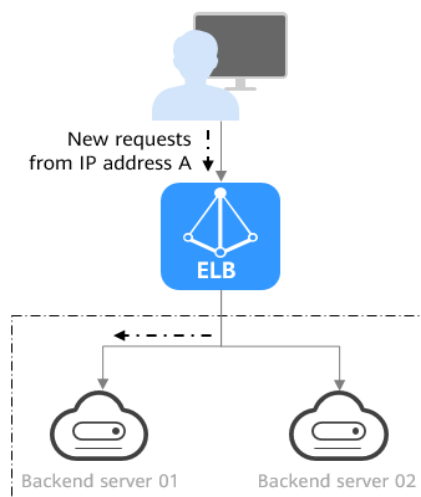


Table 1-49 Source IP hash

Description	The source IP hash algorithm calculates the source IP address of each request and routes requests from the same IP address to the same backend server.
--------------------	--

<p>When to Use</p>	<p>This algorithm is often used for applications that need to maintain user sessions or state.</p> <ul style="list-style-type: none"> • Session persistence: Source IP hash ensures that requests with the same source IP address are distributed to the same backend server. • Data consistency: Requests with the same hash value are distributed to the same backend server. • Load balancing: In scenarios that have high requirements for load balancing, this algorithm can distribute requests to balance loads among servers.
<p>Disadvantages</p>	<ul style="list-style-type: none"> • Imbalanced loads across servers: This algorithm tries its best to ensure request consistency when backend servers are added or removed. If the number of backend servers decreases, some requests may be redistributed, causing imbalanced loads across servers. • Complex calculation: This algorithm calculates the hash values of requests based on hash factors. If servers are added or removed, some requests may be redistributed, making calculation more difficult.

Connection ID

Figure 1-15 shows an example of how requests are distributed using the connection ID algorithm. Two backend servers are in the same AZ and have the same weight. If backend server 01 has processed a request from client A, the load balancer will route new requests from client A to backend server 01.

Figure 1-15 Traffic distribution using the connection ID algorithm

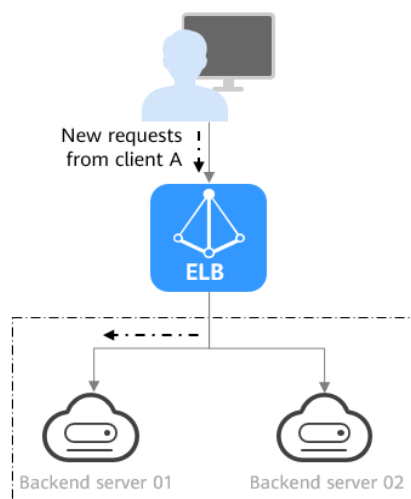


Table 1-50 Connection ID

Description	<p>The connection ID algorithm calculates the QUIC connection ID and routes requests with the same hash value to the same backend server. A QUIC ID identifies a QUIC connection. This algorithm distributes requests by QUIC connection.</p> <p>You can use this algorithm to distribute requests only to QUIC backend server groups.</p>
When to Use	<p>This algorithm is typically used for QUIC requests.</p> <ul style="list-style-type: none">● Session persistence: The connection ID algorithm ensures that requests with the same hash value are distributed to the same backend server.● Data consistency: Requests with the same hash value are distributed to the same backend server.● Load balancing: In scenarios that have high requirements for load balancing, this algorithm can distribute requests to balance loads among servers.
Disadvantages	<ul style="list-style-type: none">● Imbalanced loads across servers: This algorithm tries its best to ensure request consistency when backend servers are added or removed. If the number of backend servers decreases, some requests may be redistributed, causing imbalanced loads across servers. If the number of backend servers is small, load imbalance may occur during the reallocation.● Complex calculation: This algorithm calculates the hash values of requests based on hash factors. If servers are added or removed, some requests may be redistributed, making calculation more difficult.

Changing a Load Balancing Algorithm

1. Go to the [backend server group list page](#).
2. On the **Backend Server Groups** page, locate the target backend server group and click **Edit** in the **Operation** column.
3. In the **Modify Backend Server Group** dialog box, change the load balancing algorithm.
4. Click **OK**.

NOTE

The change is applied immediately and will be used to route requests over new connections. However, the previous load balancing algorithm will still be used to route requests over established connections.

1.5.3.2 Sticky Session

Sticky sessions ensure that requests from a client always get routed to the same backend server before a session elapses.

Here is an example that describes how sticky session works. Assume that you have logged in to a server. After a while, you send another request. If sticky sessions are not enabled, the request may be routed to another server, and you will be asked to log in again. If sticky sessions are enabled, all your requests are processed by the same server, and you do not need to repeatedly log in.

Differences Between Sticky Sessions at Layer 4 and Layer 7

The following table describes the differences of sticky sessions at Layer 4 at Layer 7.

Table 1-51 Sticky session comparison

OSI Layer	Listener Protocol	Sticky Session Type	Stickiness Duration	Scenarios Where Sticky Sessions Become Invalid
Layer 4	TCP or UDP	Source IP address: The source IP address of each request is calculated using the consistent hashing algorithm to obtain a unique hashing key, and all backend servers are numbered. The system allocates the client to a particular server based on the generated key. This allows requests from the same IP address are forwarded to the same backend server.	<ul style="list-style-type: none">• Default: 20 minutes• Maximum: 60 minutes• Range: 1 minute to 60 minutes	<ul style="list-style-type: none">• Source IP addresses of the clients change.• The session stickiness duration has been reached.

OSI Layer	Listener Protocol	Sticky Session Type	Stickiness Duration	Scenarios Where Sticky Sessions Become Invalid
Layer 7	HTTP or HTTPS	<ul style="list-style-type: none"> • Load balancer cookie: The load balancer generates a cookie after receiving a request from the client. All subsequent requests with the cookie are then routed to the same backend server. • Application cookie: The application deployed on the backend server generates a cookie after receiving the first request from the client. All subsequent requests with the cookie are routed to the same backend server. 	<ul style="list-style-type: none"> • Default: 20 minutes • Maximum: 1,440 minutes • Range: 1 minute to 1,440 minutes 	<ul style="list-style-type: none"> • If requests sent by the clients do not contain a cookie, sticky sessions will not take effect. • Requests from the clients exceed the session stickiness duration.

 **NOTE**

- If you set **Load Balancing Algorithm** to **Source IP hash**, you do not need to manually enable and configure **Sticky Session**. Source IP hash allows requests from the same client to be directed to the same server.
- If you set **Load Balancing Algorithm** to **Weighted round robin** or **Weighted least connections**, you need to manually enable and configure **Sticky Session**.

Notes and Constraints

- If you use **Cloud Connect connection**, **Direct Connect** or **VPN** to access ELB, you must select **Source IP hash** as the load balancing algorithm and disable sticky sessions for ELB.

- Dedicated load balancers support **Source IP address**, **Application cookie**, and **Load balancer cookie**.

 **NOTE**

- **Application cookie** will be available in more regions. You can see which regions support them on the console.
- For HTTP and HTTPS listeners, enabling or disabling sticky sessions may cause few seconds of service interruption.
- If you enable sticky sessions, traffic to backend servers may be unbalanced. If this happens, disable sticky sessions and check the requests received by each backend server.

Enabling or Disabling Sticky Session

1. Go to the [backend server group list page](#).
2. On the **Backend Server Groups** page, locate the backend server group and click **Edit** in the **Operation** column.
3. In the **Modify Backend Server Group** dialog box, enable or disable **Sticky Session**.
If you enable it, select the sticky session type, and set the session stickiness duration.
4. Click **OK**.

1.5.3.3 Slow Start

If you enable slow start, the load balancer linearly increases the proportion of requests to the new backend servers added to the backend server group. When the slow start duration elapses, the load balancer sends full share of requests to backend servers and exits the slow start mode. For details about how to set weights for backend servers, see [Backend Server Weights](#).

Slow start gives applications time to warm up and respond to requests with optimal performance.

 **NOTE**

Slow start is only available for HTTP and HTTPS backend server groups of dedicated load balancers.

Backend servers will exit slow start in either of the following cases:

- The slow start duration elapses.
- Backend servers become unhealthy during the slow start duration.

Notes and Constraints

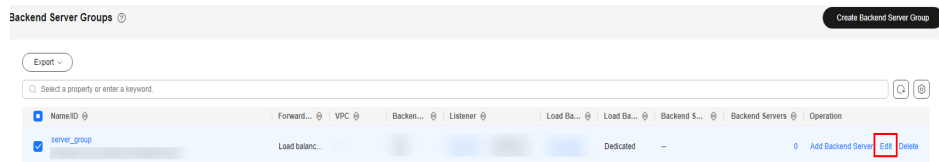
- Weighted round robin must be selected as the load balancing algorithm.
- Slow start takes effect only for new backend servers and does not take effect when the first backend server is added to a backend server group.
- After the slow start duration elapses, backend servers will not enter the slow start mode again.
- Slow start takes effect when health check is enabled and the backend servers are running normally.

- If health check is disabled, slow start takes effect immediately.

Enabling or Disabling Slow Start

1. Go to the [backend server group list page](#).
2. On the **Backend Server Groups** page, locate the backend server group and click **Edit** in the **Operation** column.

Figure 1-16 Modifying a backend server group



3. In the **Modify Backend Server Group** dialog box, enable or disable **Slow Start**.
If you enable it, you need to set the slow start duration. The duration ranges from 30 to 1200. When the slow start duration elapses, the load balancer sends full share of requests to backend servers and exits slow start.
4. Click **OK**.

1.5.4 Changing a Backend Server Group

Scenario

This section describes how you can change the default backend server group configured for a listener.

TCP, TLS, or UDP listeners forward requests to the default backend server groups.

HTTP, QUIC, or HTTPS listeners forward requests based on the priorities of the forwarding policies. If you do not add a forwarding policy, the listener will route the requests to the default backend server group.

Notes and Constraints

- The backend server group cannot be changed if redirection is enabled.
- The backend protocol of the backend server group must match the frontend protocol of the listener. For details, see [Table 1-41](#).

Procedure

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the target load balancer and click its name.
3. On the **Listeners** tab, locate the target listener and click its name.
4. On the **Summary** tab, click **Change Backend Server Group** on the right of **Default Backend Server Group** area.
5. In the displayed dialog box, click the server group name box.
Select a backend server group from the drop-down list or create a group.

- a. Click the name of the backend server group or enter the name in the search box to search for the target group.
- b. Click **Create Backend Server Group**. After the backend server group is created, click the refresh icon.

 **NOTE**

The backend protocol of the new backend server group must match the frontend protocol of the listener.

6. Click **OK**.

1.5.5 Managing a Backend Server Group

You can manage a backend server group as required.

Enabling Modification Protection

You can enable the modification protection option for a backend server group to prevent the backend servers in it from being modified or deleted by accident.

Enabling the modification protection option for a backend server group will prohibit any change to both the group and the backend servers in it.

1. Go to the [backend server group list page](#).
2. On the **Backend Server Groups** page, locate the backend server group and click its name.
3. On the **Summary** tab, click **Configure** next to **Modification Protection**.
4. In the **Configure Modification Protection** dialog box, enable **Modification Protection**.
5. Click **OK**.

 **NOTE**

Disable **Modification Protection** if you want to delete a backend server group or modify its settings.

Viewing a Backend Server Group

You can view the details of a backend server group.

1. Go to the [backend server group list page](#).
2. On the **Backend Server Groups** page, click the name of the backend server group.
3. Click different tabs to view the required information.
 - a. On the **Summary** tab, view the basic information (name, ID, backend protocol) and health check settings.
 - b. On the **Backend Servers** tab, view the servers that have been added to the backend server group.
 - c. On the **Associated Resources** tab, view the resources (load balancers, listeners, and forwarding policies) that are associated with the backend server group.

Deleting a Backend Server Group

Before deleting a backend server group, you need to:

- Disassociate it from the listener. For details, see [Changing a Backend Server Group](#).
 - Ensure the backend server group is not used by a forwarding policy of an HTTP or HTTPS listener.
1. Go to the [backend server group list page](#).
 2. On the **Backend Server Groups** page, locate the backend server group and click **Delete** in the **Operation** column.
 3. In the displayed dialog box, click **OK**.

1.6 Backend Server

1.6.1 Backend Server Overview

Backend servers receive and process requests from the associated load balancer.

If the incoming traffic increases, you can add more backend servers to ensure the stability and reliability of applications and eliminate SPOFs. If the incoming traffic decreases, you can remove some backend servers to reduce the cost.

If the load balancer is associated with an AS group, instances are automatically added to or removed from the load balancer.

Different types of backend servers can be added to different types of backend server groups as described in [Table 1-52](#).

Table 1-52 Backend server group and backend server types

Backend Server Group Type	Backend Server Types	Reference
Hybrid	<ul style="list-style-type: none">• Cloud servers or supplementary network interfaces that are in the same VPC as the load balancer, if IP as a Backend is disabled• IP addresses of servers in other VPCs or in your on-premises data center, if IP as a Backend is enabled <p>NOTE When you create a hybrid backend server group, you must specify a VPC and associate the backend server group with a load balancer in this VPC.</p>	<ul style="list-style-type: none">• Adding Backend Servers in the Same VPC as a Load Balancer• Adding Backend Servers in a Different VPC from a Load Balancer

Backend Server Group Type	Backend Server Types	Reference
IP as a backend server	IP addresses of cloud or on-premises servers NOTE IP as a Backend must have been enabled for the load balancer.	Adding Backend Servers in a Different VPC from a Load Balancer

Precautions

- It is recommended that you select backend servers running the same OS for easier management and maintenance.
- The load balancer checks the health of each server added to the associated backend server group if you have configured health check for the backend server group. If the backend server responds normally, the load balancer will consider it healthy. If the backend server does not respond normally, the load balancer will periodically check its health until the backend server is considered healthy.
- If a backend server is stopped or restarted, connections established with the server will be disconnected, and data being transmitted over these connections will be lost. To avoid this from happening, configure the retry function on the clients to prevent data loss.
- If you enable sticky sessions, traffic to backend servers may be unbalanced. If this happens, disable sticky sessions and check the requests received by each backend server.
- You can adjust the number of backend servers associated with a load balancer at any time. You can also change the type of backend servers according to your service needs. To ensure service stability, ensure that the load balancer can perform health checks normally, and at least one backend server that is running properly has been added to the load balancer.

Notes and Constraints

- A maximum of 500 backend servers can be added to a backend server group.
- Inbound security group rules must be configured to allow traffic over the port of each backend server and health check port. For details, see [Security Group and Network ACL Rules](#).
- If you select only network load balancing, a server cannot serve as both a backend server and a client.

Backend Server Weights

You need to set a weight for each backend server in a backend server group to receive requests. The higher the weight you have configured for a backend server, the more requests the backend server receives.

You can set an integer from **0** to **100**. If you set the weight of a backend server to **0**, new requests will not be routed to this server.

Three load balancing algorithms allow you to set weights to backend servers, as shown in the following table. For more information about load balancing algorithms, see [Load Balancing Algorithms](#).

Table 1-53 Server weights in different load balancing algorithms

Load Balancing Algorithm	Weight Setting
Weighted round robin	<ul style="list-style-type: none">• If none of the backend servers have a weight of 0, the load balancer routes requests to backend servers based on their weights. Backend servers with higher weights receive proportionately more requests.• If two backend servers have the same weights, they receive the same number of requests.
Weighted least connections	<ul style="list-style-type: none">• If none of the backend servers have a weight of 0, the load balancer calculates the load of each backend server using the formula (Overhead = Number of current connections/Backend server weight).• The load balancer routes requests to the backend server with the lowest overhead.
Source IP hash	<ul style="list-style-type: none">• If none of the backend servers have a weight of 0, requests from the same client are routed to the same backend server within a period of time.• If the weight of a backend server is 0, no requests are routed to this backend server.

1.6.2 Security Group and Network ACL Rules

Scenarios

To ensure normal communications between the load balancer and backend servers, you need to check the security group and network ACL rules.

- Security group rules of backend servers must allow traffic from the backend subnet where the load balancer is created to the backend servers. (By default, the backend subnet of a load balancer is the same as the subnet where the load balancer works.) For details about how to configure security group rules, see [Configuring Security Group Rules](#).
- Network ACL rules are optional for subnets. If network ACL rules are configured for the subnet where the backend servers are deployed, the rules must allow traffic from the backend subnet of the load balancer to the subnet of the backend servers. For details about how to configure network ACL rules, see [Configuring Network ACL Rules](#).

 NOTE

If the dedicated load balancer has a Layer-4 listener and IP as a backend is disabled, security group and network ACL rules will not work.

You can use access control to limit which IP addresses are allowed or denied to access the listener. For details, see [What Is Access Control?](#)

Notes and Constraints

- If health check is enabled for a backend server group, security group rules must allow traffic from the health check port over the health check protocol.
- If UDP is used for health check, there must be a rule that allows ICMP traffic to check the health of the backend servers.

Configuring Security Group Rules

If you have no VPCs when creating a server, the system automatically creates one for you. Default security group rules allow only communications among the servers in the VPC. To ensure that the load balancer can communicate with these servers over both the frontend port and health check port, configure inbound rules for security groups containing these servers.



1. Log in to the management console.
2. In the upper left corner of the page, click  and select the desired region and project.
3. Click  in the upper left corner to display **Service List** and choose **Compute > Elastic Cloud Server**.
4. In the ECS list, click the name of the ECS whose security group rules you want to modify.
The ECS details page is displayed.
5. Click **Security Groups**, locate the security group, and view security group rules.
6. Click the ID of a security group rule or **Modify Security Group Rule**. The security group details page is displayed.
7. On the **Inbound Rules** tab, click **Add Rule**. Configure inbound rules based on [Table 1-54](#).

Table 1-54 Security group rules

Backend Protocol	Policy	Protocol & Port	Source IP Address
HTTP or HTTPS	Allow	Protocol: TCP Port: the port used by the backend server and health check port	Backend subnet of the load balancer

Backend Protocol	Policy	Protocol & Port	Source IP Address
TCP	Allow	Protocol: TCP Port: health check port	
UDP	Allow	Protocol: UDP and ICMP Port: health check port	

 **NOTE**

- After a load balancer is created, do not change the subnet. If the subnet is changed, the IP addresses occupied by the load balancer will not be released, and traffic from the previous backend subnet is still need to be allowed to backend servers.
- Traffic from the new backend subnet is also need to be allowed to backend servers.



8. Click **OK**.

Configuring Network ACL Rules

To control traffic in and out of a subnet, you can associate a network ACL with the subnet. Network ACL rules control access to subnets and add an additional layer of defense to your subnets.

The default network rule denies all inbound and outbound traffic. You can configure an inbound rule to allow traffic from the backend subnet of the load balancer through the port of the backend server.

- If the load balancer is in the same subnet as the backend servers, network ACL rules will not take effect. In this case, the backend servers will be considered healthy and can be accessed by the clients.
- If the load balancer is not in the same subnet as the backend servers, network ACL rules will take effect. In this case, the backend servers will be considered unhealthy and cannot be accessed by the clients.

1. Log in to the management console.
2. In the upper left corner of the page, click  and select the desired region and project.
3. Click  in the upper left corner to display **Service List** and choose **Networking > Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control > Network ACLs**.
5. In the network ACL list, locate the target network ACL and click its name.
6. On the **Inbound Rules** or **Outbound Rules** tab, click **Add Rule** to add an inbound or outbound rule.
 - **Action:** Select **Allow**.

- **Type:** Select the same type as the backend subnet of the load balancer.
 - **Protocol:** The protocol must be the same as the backend protocol.
 - **Source:** Set it to the backend subnet of the load balancer.
 - **Source Port Range:** Select a port range.
 - **Destination:** Enter a destination address allowed in this direction. The default value is **0.0.0.0/0**, which indicates that traffic from all IP addresses is permitted.
 - **Destination Port Range:** Select a port range.
 - (Optional) **Description:** Describe the network ACL rule.
7. Click **OK**.

1.6.3 Adding Backend Servers in the Same VPC as a Load Balancer

When you use ELB to route requests, ensure that at least one backend server is healthy and can process requests routed by the load balancer.

If the incoming traffic increases, you can add more cloud servers to ensure the stability and reliability of applications and eliminate SPOFs. If the incoming traffic decreases, you can remove some backend servers to reduce the cost.

You can add ECSs, BMSs, and supplementary network interfaces in the VPC where the dedicated load balancer is created.

Notes and Constraints

- Cloud servers and supplementary network interfaces can only be added to a hybrid backend server group.
- Only ECSs, BMSs, and supplementary network interfaces in the same VPC as the backend server group can be added.
- Dedicated load balancers have compatibility requirements on BMS flavors. Only BMSs with **certain flavors** can be added as backend servers.

Procedure

1. Go to the [backend server group list page](#).
2. On the **Backend Server Groups** page, click the name of the target backend server group.
3. Click the **Backend Servers** tab and add servers as required.
 - a. Cloud servers (ECSs or BMSs): Locate the **Cloud Servers** area and click **Add** on the right. On the displayed page, search for the cloud servers by keyword and then add the private IP address. If you use private IP addresses for search, you can select the private IP address bound to either the primary or extended network interface.
 - b. Supplementary network interfaces: Locate the **Supplementary Network Interfaces** area and click **Add** on the right. On the displayed page, search for the supplementary network interfaces by keyword.
4. Select the servers you want to add and click **Next**.
5. Specify the weights and ports for the servers and click **Finish**.

You can set ports and weights in batches.

Modifying the Port and Weight of a Backend Server

The server weight ranges from **0** to **100**. If you set the weight of a cloud server to **0**, new requests will not be routed to this server.

The weights can only be specified when you select weighted round robin, weighted least connections, or source IP hash as the load balancing algorithm. For more information about load balancing algorithms, see [Backend Server Weights](#).

1. Go to the [backend server group list page](#).
2. On the **Backend Server Groups** page, click the name of the target backend server group.
3. On the **Backend Servers** tab, click **Cloud Servers** or **Supplementary Network Interfaces**.
4. Select the target backend servers and click **Modify Port/Weight** up above the backend server list.
5. In the displayed dialog box, modify ports/weights as you need.
 - Modifying ports:
 - Modifying the port of a cloud server: Set the port in the **Backend Port** column.
 - Modifying the ports of multiple cloud servers: Set the port next to **Batch Modify Ports** and click **OK**.
 - Modifying weights:
 - Modifying the weight of a cloud server: Set the weight in the **Weight** column.
 - Modifying the weights of multiple cloud servers: Set the weight next to **Batch Modify Weights** and click **OK**.
6. Click **OK**.

NOTE

You can set the weights of multiple cloud servers to **0** to block them from receiving requests routed by each load balancer.

Removing a Cloud Server

If a cloud server is removed, it is disassociated from the load balancer and can still run normally. However, it cannot receive requests from the load balancer. You can add this cloud server to the backend server group again when traffic increases or the reliability needs to be enhanced.

NOTE

If a cloud server is removed, requests are still routed to it. This is because a persistent connection is established between the load balancer and the cloud server and requests are routed to this server until the TCP connection times out. If no data is transmitted over this TCP connection after it times out, ELB disconnects the connection.

1. Go to the [backend server group list page](#).

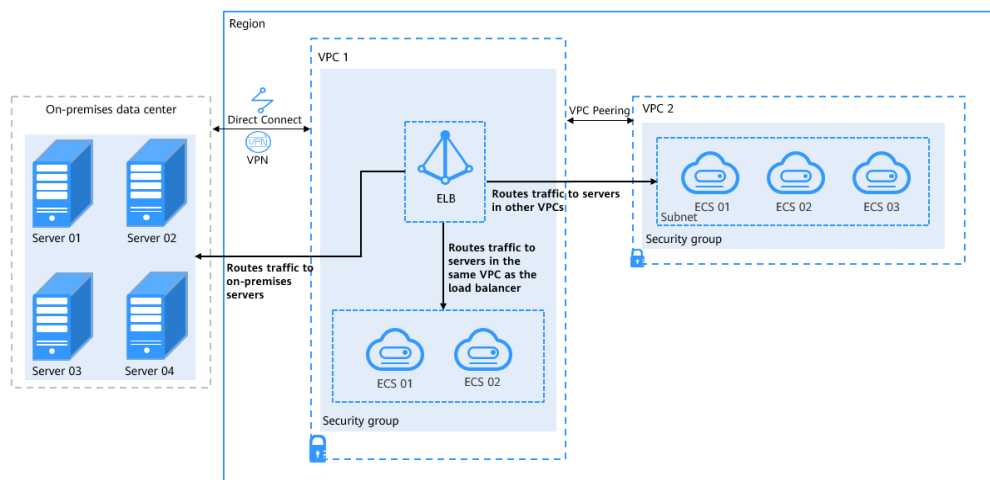
2. On the **Backend Server Groups** page, click the name of the target backend server group.
3. Switch to the **Backend Servers** tab and click **Cloud Servers** or **Supplementary Network Interfaces**.
4. Select the backend servers you want to remove and click **Remove** above the backend server list.
5. In the displayed dialog box, click **OK**.

1.6.4 Adding Backend Servers in a Different VPC from a Load Balancer

Dedicated load balancers can distribute traffic across cloud servers and on-premises servers. You can add cloud servers and supplementary network interfaces in the VPC where the dedicated load balancer is created. After enabling IP as a backend, you can also add the IP addresses of servers in other VPCs or in your on-premises data center.

In this way, incoming traffic can be flexibly distributed to cloud servers and on-premises servers.

Figure 1-17 Routing requests to cloud and on-premises servers



Notes and Constraints

- **IP as a Backend** cannot be disabled after it is enabled.
- Before forwarding requests to servers in other VPCs, ensure that the target VPC can communicate with the VPC where the load balancer is created.
- Only private IPv4 addresses can be added as backend servers.
- A maximum of 100,000 concurrent connections can be established with a backend server that is added by using its IP address.
- If you add IP addresses as backend servers, the source IP addresses of the clients cannot be passed to these servers. Install the **TOA module** to obtain source IP addresses.

Distributing Traffic Across IP as Backend Servers

With a wide variety of networking services, you can flexibly connect VPCs in the same region, in different regions, or in different accounts.

After VPCs where IP as backend servers are running are connected, traffic can be distributed across these backend servers.

For details about the network connectivity options, see [VPC Connectivity Options](#).

Table 1-55 Distributing traffic across IP as backend servers

Where Servers Are Running	Networking Service	Function	Reference
Different VPCs in the same region	VPC Peering	With VPC Peering, you can peer two VPCs in the same region. The VPCs can be in the same account or different accounts.	Using a VPC Peering Connection to Connect Two VPCs
	Enterprise Router	An enterprise router can connect multiple VPCs in the same account or different accounts to set up a hub-and-spoke network. Compared with VPC Peering, Enterprise Router is more suitable for complex networking where many VPCs need to be connected.	Using Enterprise Router to Connect VPCs in the Same Region

Where Servers Are Running	Networking Service	Function	Reference
Different VPCs in different regions	Cloud Connect <ul style="list-style-type: none"> • Cloud connections • Central networks 	Cloud Connect can connect VPCs in the same account or different accounts across regions. Cloud Connect provides the following two options: <ul style="list-style-type: none"> • Cloud connection: Load VPCs in different regions to a cloud connection. • Central network: Attach VPCs in the same region to an enterprise router, and add enterprise routers in different regions to a central network as attachments. This solution features higher scalability and is suitable for complex networking with many VPCs from different regions. 	<ul style="list-style-type: none"> • Using a Cloud Connection to Connect VPCs in Different Regions • Using a Central Network and Enterprise Routers to Connect VPCs in Different Regions
	VPN	VPN allows VPCs in different regions to communicate with each other over the Internet.	Using VPN to Connect VPCs Across Regions
	Direct Connect	VPCs in different regions can be connected through Direct Connect connections.	Using Direct Connect to Connect VPCs in Different Regions
On-premises data centers	VPN	VPN connects on-premises data centers and VPCs over the Internet.	Configuring Enterprise Edition S2C VPN to Connect an On-premises Data Center to a VPC
	Direct Connect	You can use Direct Connect to connect a VPC to an on-premises data center.	Using Direct Connect to Connect an On-premises Data Center to the Cloud

Enabling IP as a Backend

1. Go to the [load balancer list page](#).
2. On the load balancer list page, click the name of the target load balancer.
3. On the **Summary** tab, click **Enable** next to **IP as a Backend**.
4. Click **OK**.

Adding IP as Backend Servers

1. Go to the [backend server group list page](#).
2. On the **Backend Server Groups** page, click the name of the target backend server group.
3. Switch to the **Backend Servers** tab and click **Add** above the IP address as backend server list.
4. Specify the IP addresses, backend ports, and weights.
5. Click **OK**.

Modifying the Ports/Weights of IP as Backend Servers

The server weight ranges from **0** to **100**. If you set the weight to **0**, new requests will not be routed to this server.

The weights can only be specified when you select weighted round robin, weighted least connections, or source IP hash as the load balancing algorithm. For more information about load balancing algorithms, see [Backend Server Weights](#).

NOTE

Only certain regions support backend port modification. See the details on the management console.

1. Go to the [backend server group list page](#).
2. On the **Backend Server Groups** page, click the name of the target backend server group.
3. Switch to the **Backend Servers** tab and click **IP as Backend Servers**.
4. Select the servers and click **Modify Port/Weight** up the server list.
5. In the displayed dialog box, modify ports/weights as you need.
 - Modifying ports:
 - Modifying the port of an IP as backend server: Set the port in the **Backend Port** column.
 - Modifying the ports of multiple IP as backend servers: Set the port next to **Batch Modify Ports**, and click **OK**.
 - Modifying weights:
 - Modifying the weight of an IP as backend server: Set the weight in the **Weight** column.
 - Modifying the weights of multiple IP as backend servers: Set the weight next to **Batch Modify Weights** and click **OK**.

 NOTE

You can set the weights of multiple servers to **0** to block them from receiving requests routed by each load balancer.

6. Click **OK**.

Removing IP as Backend Servers

 NOTE

If a cloud server is removed, requests are still routed to it. This is because a persistent connection is established between the load balancer and the cloud server and requests are routed to this server until the TCP connection times out. If no data is transmitted over this TCP connection after it times out, ELB disconnects the connection.

1. Go to the [backend server group list page](#).
2. On the **Backend Server Groups** page, click the name of the target backend server group.
3. Switch to the **Backend Servers** tab and click **IP as Backend Servers**.
4. Select the IP as backend servers to be removed and click **Remove** above the server list.
5. In the displayed dialog box, click **OK**.

1.7 Health Check

1.7.1 Health Check

ELB periodically sends requests to backend servers to check whether they can process requests. This process is called health check.

If a backend server is detected unhealthy, the load balancer will stop routing requests to it. After the backend server recovers, the load balancer will resume routing requests to it.

If backend servers have to handle large number of requests, frequent health checks may overload the backend servers and cause them to respond slowly. To address this problem, you can prolong the health check interval or use TCP or UDP instead of HTTP. You can also disable health check. If you choose to disable health check, requests may be routed to unhealthy servers, and service interruptions may occur.

Health Check Protocol

You can configure health checks when configuring backend server groups. Generally, you can use the default setting or select a different health check protocol as you need.

If you want to modify health check settings, see details in [Configuring a Health Check](#).

Select a health check protocol that matches the backend protocol as described in [Table 1-56](#).

Table 1-56 The backend protocol and health check protocols (dedicated load balancers)

Backend Protocol	Health Check Protocol
TCP	TCP, HTTP, or HTTPS
UDP	UDP
QUIC	UDP
TLS	TCP, HTTP, TLS, gRPC, or HTTPS
HTTP	TCP, HTTP, TLS, gRPC, or HTTPS
HTTPS	TCP, HTTP, TLS, gRPC, or HTTPS
gRPC	TCP, HTTP, TLS, gRPC, or HTTPS

 **NOTE**

TLS and gRPC are available in certain regions. You can see which regions support them on the console.

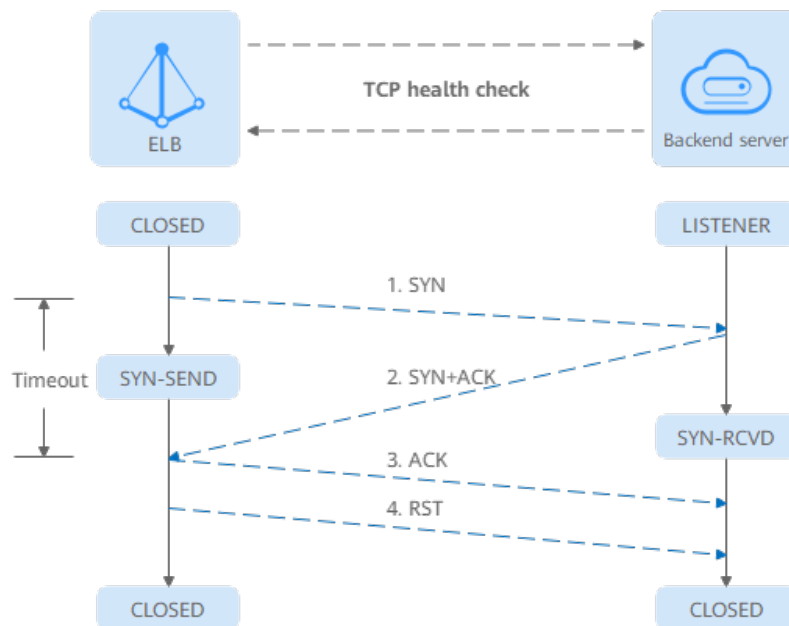
Health Check Source IP Address

A dedicated load balancer uses the IP addresses in its backend subnet to send requests to backend servers and verify their health status. To perform health checks, ensure that the security group rules of the backend servers allow access from the backend subnet where the load balancer works. For details, see [Security Group and Network ACL Rules](#).

TCP Health Check

For TCP, HTTP, and HTTPS backend protocols, you can use TCP to initiate three-way handshakes to obtain the statuses of backend servers.

Figure 1-18 TCP health check



The TCP health check process is as follows:

1. The load balancer sends a TCP SYN packet to the backend server (in the format of $\{Private\ IP\ address\};\{Health\ check\ port\}$).
2. The backend server returns an SYN-ACK packet.
 - If the load balancer does not receive the SYN-ACK packet within the timeout duration, it declares that the backend server is unhealthy and sends an RST packet to the backend server to terminate the TCP connection.
 - If the load balancer receives the SYN-ACK packet from the backend server within the timeout duration, it sends an ACK packet to the backend server and declares that the backend server is healthy. After that, the load balancer sends an RST packet to the backend server to terminate the TCP connection.

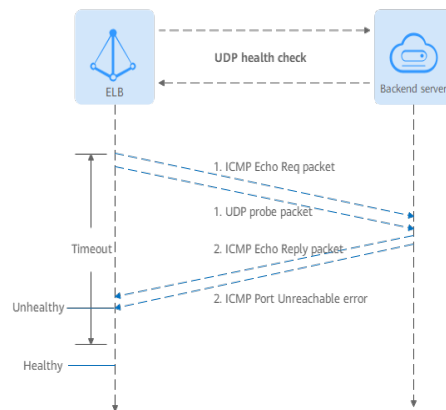
NOTICE

After a successful TCP three-way handshake, an RST packet will be sent to close the TCP connection. The application on the backend server may consider this packet a connection error and reply with a message, for example, "Connection reset by peer". To avoid this issue, take either of the following actions:

- Use [HTTP Health Check](#).
- Have the backend server ignore the connection error.

UDP Health Check

For UDP backend protocol, ELB sends ICMP and UDP probe packets to backend servers to check their health.

Figure 1-19 UDP health check

The UDP health check process is as follows:

1. The load balancer sends an ICMP Echo Request packet and UDP probe packet to the backend server.
2. If the load balancer receives an ICMP Echo Reply packet and does not receive an ICMP Port Unreachable error within the health check timeout duration, it considers the backend server as healthy. If the load balancer receives an ICMP Port Unreachable error, it considers the backend server as unhealthy.

NOTE

- If there is a large number of concurrent requests, the health check result may be different from the actual health of the backend server.
If the backend server runs Linux, it may limit the rate of ICMP packets as a defense against ping flood attacks. In this case, even if there is a service exception, ELB will not receive the error message "port XX unreachable", and the server will still be determined healthy. This causes the health check result to be different from the actual health of the backend server.
- The UDP probe packet's payload has no significance and is simply used to fill the packet with data. Typically, the payload is set to "H". Clients should not attempt to interpret its content.

HTTP Health Check

You can also configure HTTP health checks to obtain server statuses through HTTP GET requests if you select TCP, HTTP, or HTTPS as the backend protocol. [Figure 1-20](#) shows how an HTTP health check works.

Figure 1-20 HTTP health check

The HTTPS health check process is as follows:

1. The load balancer sends an HTTP GET request to the backend server (in format of *{Private IP address}:{Health check port}/{Health check path}*). (You can specify a domain name when configuring a health check.)
2. The backend server returns an HTTP status code to ELB.
 - If the load balancer receives the status code within the health check timeout duration, it compares the status code with the preset one. If the status codes are the same, the backend server is declared healthy.
 - If the load balancer does not receive any response from the backend server within the health check timeout duration, it declares the backend server is unhealthy.

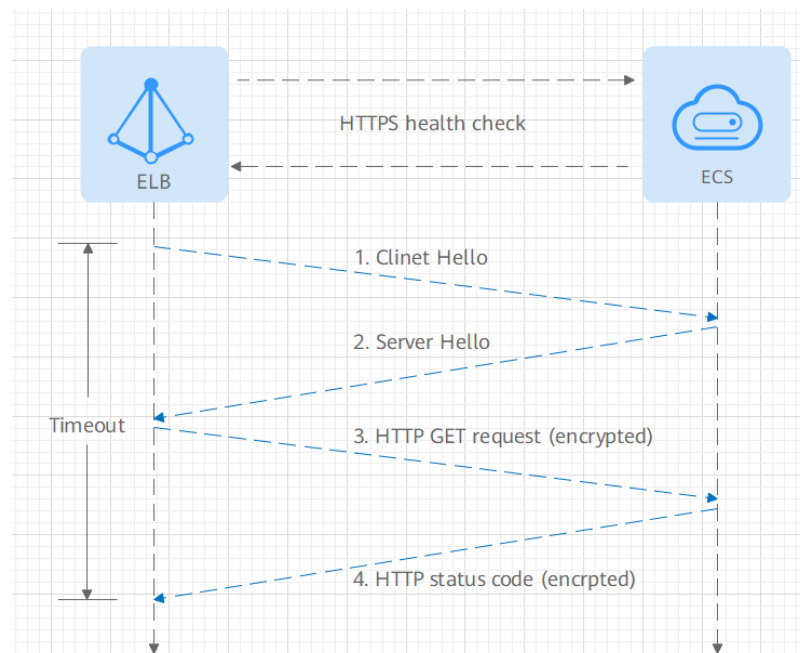
NOTE

- If HTTP health check is selected for the TCP listener of a dedicated load balancer, the load balancer uses HTTP/1.0 to send requests to backend servers. HTTP/1.0 is used to establish short-lived connections. This means the load balancer will not translate the HTTP responses until it receives the TCP disconnection packet. Ensure that the backend server disconnects the TCP connection immediately after sending the responses. Otherwise, the health check may fail.
- In an HTTP health check, the User-Agent header identifies that the requests are sent for health checks. The value of User-Agent may be adjusted based on service requirements. So, it is not recommended to rely on this header for verification or judgment.
- If the private IP address of a backend server is used as the domain name for a health check, do not rely on the host header for verification or judgment, as it may be empty.

HTTPS Health Check

For TCP, HTTP, and HTTPS backend protocols, you can use HTTPS to establish an SSL connection over TLS handshakes to obtain the statuses of backend servers.

Figure 1-21 shows how an HTTPS health check works.

Figure 1-21 HTTPS health check

The HTTPS health check process is as follows:

1. The load balancer sends a Client Hello packet to establish an SSL connection with the backend server.
2. After receiving the Server Hello packet from the backend server, the load balancer sends an encrypted HTTP GET request to the backend server (in the format of *{Private IP address}:{Health check port}/{Health check path}*). (You can specify a domain name when configuring a health check.)
3. The backend server returns an HTTP status code to the load balancer.
 - If the load balancer receives the status code within the health check timeout duration, it compares the status code with the preset one. If the status codes are the same, the backend server is declared healthy.
 - If the load balancer does not receive any response from the backend server within the health check timeout duration, it declares the backend server is unhealthy.

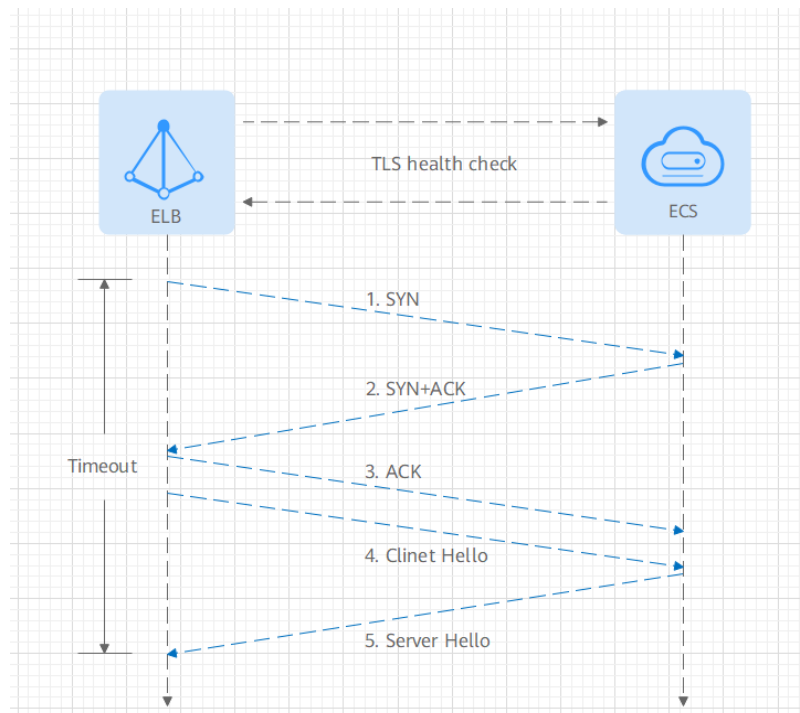
NOTE

- In an HTTPS health check, the User-Agent header identifies that the requests are sent for health checks. The value of User-Agent may be adjusted based on service requirements. So, it is not recommended to rely on this header for verification or judgment.
- If the private IP address of a backend server is used as the domain name for a health check, do not rely on the host header for verification or judgment.

TLS Health Check

For the TLS, HTTP, and HTTPS backend protocols, you can use TLS to initiate handshakes, and then send Client Hello to a backend server to check whether the server is healthy.

Figure 1-22 TLS Health Check



The TLS health check process is as follows:

1. The load balancer sends a TCP SYN packet to the backend server (in the format of $\{Private\ IP\ address\}:\{Health\ check\ port\}$).
 - If the load balancer does not receive the SYN-ACK packet within the health check timeout duration, the backend server is declared unhealthy.
 - If the load balancer receives an SYN+ACK packet within the timeout duration, it sends a Client Hello packet to the backend server. The TLS versions include TLSv1.0, TLSv1.1, TLSv1.2, and TLSv1.3.
2. If the load balancer receives the Server Hello packet within the timeout duration, the backend server is declared healthy. If the load balancer does not receive the Server Hello packet within the timeout duration, it declares the backend server is unhealthy.

gRPC Health Check

Figure 1-23 gRPC health check



The gRPC health check process is as follows:

1. The load balancer sends an HTTP POST or GET request to the backend server (in format of *{Private IP address}:{Health check port}/{Health check path}*). (You can specify a domain name when configuring a health check.)
2. The backend server returns a status code to the load balancer.
3. The load balancer receives the value of `grpc-status` in the HTTP/2 header as the returned gRPC status code.
 - If the load balancer receives the status code within the health check timeout duration, it compares the status code with the preset one. If the status codes are the same, the backend server is declared healthy.
 - If the load balancer does not receive any response from the backend server within the health check timeout duration, it declares the backend server is unhealthy.

Health Check Time Window

Health checks greatly improve service availability. However, if health checks are too frequent, service availability will be compromised. To avoid the impact, ELB declares a backend server healthy or unhealthy after several consecutive health checks.

The health check time window is determined by the factors in [Table 1-57](#).

Table 1-57 Factors affecting the health check time window

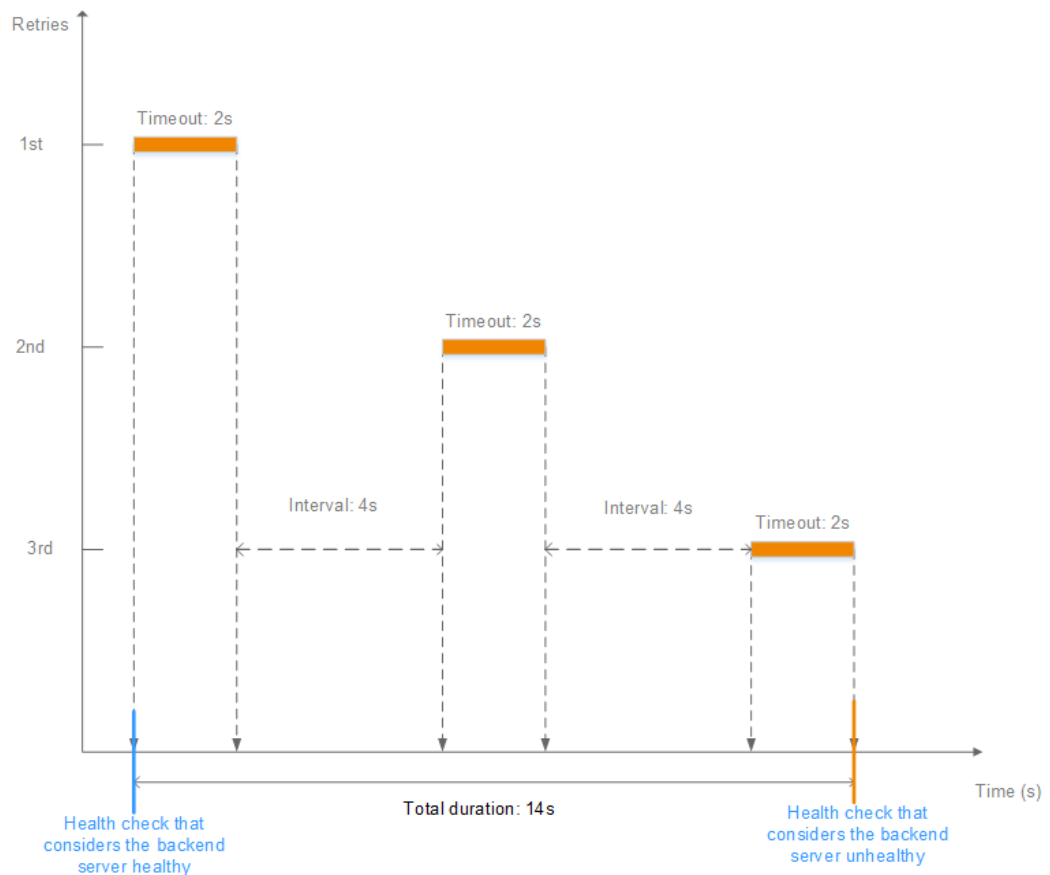
Factor	Description
Check Interval	How often health checks are performed.
Timeout Duration	How long the load balancer waits for the response from the backend server.
Health Check Threshold	The number of consecutive successful or failed health checks required for determining whether the backend server is healthy or unhealthy.

The following is a formula for you to calculate the health check time window:

- Time window for a backend server to be detected healthy = Timeout duration x Healthy threshold + Interval x (Healthy threshold - 1)
- Time window for a backend server to be detected unhealthy = Timeout duration x Unhealthy threshold + Interval x (Unhealthy threshold - 1)

As shown in [Figure 1-24](#), if the health check interval is 4s, the health check timeout duration is 2s, and unhealthy threshold is 3, the time window for a backend server to be considered unhealthy is calculated as follows: $2 \times 3 + 4 \times (3 - 1) = 14s$.

Figure 1-24 Health check timeout window



Rectifying an Unhealthy Backend Server

If a backend server is detected unhealthy, see [How Do I Troubleshoot an Unhealthy Backend Server?](#)

1.7.2 Configuring a Health Check

Scenarios

This section describes how you can enable or disable the health check option.

After the protocol is changed, the load balancer uses the new protocol to check the health of backend servers. The load balancer continues to route traffic to the backend servers after they are detected healthy.

Before the new configurations take effect, the load balancer may return the HTTP 503 error code to the clients.

Notes and Constraints

- The health check protocol can be different from the backend protocol.
- To reduce the vCPU usage of the backend servers, it is recommended that you use TCP for health checks. If you want to use HTTP for health checks, you can use static files to return the health check results.

- If health check is enabled, security group rules must allow traffic from the health check port to the backend servers over the health check protocol. For details, see [Security Group and Network ACL Rules](#).

NOTE

After you enable health check, the load balancer immediately checks the health of backend servers.

- If a backend server is detected healthy, the load balancer will start routing requests to it over new connections based on the configured loading balancing algorithms and weights.
- If a backend server is detected unhealthy, the load balancer will stop routing traffic to it.

Enabling Health Check

1. Go to the [backend server group list page](#).
2. On the **Backend Server Groups** page, locate the backend server group and click its name.
3. On the **Summary** page, click **Health Check** on the right.
4. In the **Configure Health Check** dialog box, configure the parameters based on [Table 1-58](#).

Table 1-58 Parameters required for configuring health check

Parameter	Description	Example Value
Health Check	Specifies whether to enable health checks. NOTE When the health check is enabled or disabled, the number of healthy or unhealthy backend servers may temporarily fluctuate but will stabilize after a monitoring period.	N/A
Health Check Protocol	Specifies the protocol that will be used by the load balancer to check the health of backend servers. If the protocol of the backend server group is UDP, the health check protocol is UDP by default. Dedicated load balancers support TCP, HTTP, TLS, gRPC, and HTTPS.	HTTP

Parameter	Description	Example Value
Domain Name	<p>Specifies the domain name that will be used for health checks. This parameter is mandatory if the health check protocol is HTTP, gRPC, or HTTPS.</p> <ul style="list-style-type: none">You can use the private IP address of the backend server as the domain name.You can also specify a domain name that consists of at least two labels separated by periods (.). Use only letters, digits, and hyphens (-). Do not start or end strings with a hyphen. Max total: 100 characters. Max label: 63 characters.	www.elb.com
Health Check Port	<p>Specifies the port that will be used by the load balancer to check the health of backend servers. The port number ranges from 1 to 65535.</p> <p>NOTE By default, the service port on each backend server is used. You can also specify a port for health checks.</p>	80
Path	<p>Specifies the health check URL, which is the destination on backend servers for health checks. This parameter is mandatory if the health check protocol is HTTP, gRPC, or HTTPS. The path can contain 1 to 80 characters and must start with a slash (/).</p> <p>If the backend server group is associated with a dedicated load balancer, the check path can contain letters, digits, hyphens (-), slashes (/), periods (.), question marks (?), number signs (#), percent signs (%), ampersands (&), and extended character sets <code>_-~!.() *[]@\$^:'!+,</code></p>	/index.html
Interval (s)	<p>Specifies the maximum time between two consecutive health checks, in seconds.</p> <p>The interval ranges from 1 to 50.</p>	5

Parameter	Description	Example Value
Timeout (s)	Specifies the maximum time required for waiting for a response from the health check, in seconds. The value ranges from 1 to 50 .	3
Healthy Threshold	Specifies the number of consecutive successful health checks required for declaring a backend server healthy. The value ranges from 1 to 10 .	3
Unhealthy Threshold	Specifies the number of consecutive failed health checks required for declaring a backend server unhealthy. The value ranges from 1 to 10 .	3
Status Code	<p>Specifies the status codes that will be returned to the load balancer to indicate the health of backend servers. This parameter is available only when you set the health check protocol to HTTP, gRPC, or HTTPS.</p> <p>You can enter a unique number or a positive number range within the status code range, for example, 0-10 and 200-300. A maximum of five HTTP status codes are supported. If there is more than one status code, press Enter to separate them.</p> <ul style="list-style-type: none">• If the check protocol is HTTP or HTTPS, the status code ranges from 200 to 599.• When the gRPC protocol is used, the status code ranges from 0 to 99. <p>NOTE This feature will be available in more regions. See details on the management console.</p>	200

5. Click **OK**.

Disabling Health Check

1. Go to the [backend server group list page](#).

2. On the **Backend Server Groups** page, click the name of the target backend server group.
3. On the **Summary** page, click **Health Check** on the right.
4. In the **Configure Health Check** dialog box, disable health check.
5. Click **OK**.

1.8 Security

1.8.1 Transfer Client IP Address

Overview

Transfer Client IP Address enables your load balancers to use the IP address of the client to access the backend servers.

[Table 1-59](#) lists whether you can enable or disable this feature.

Table 1-59 Transfer client IP address support

Listener Type	Enabling Transfer Client IP Address	Disabling Transfer Client IP Address
TCP/UDP	Enabled by default	Not supported
HTT/HTTPS/QUIC	Enabled by default	Not supported
TLS	Not supported	Not supported

Notes and Constraints

- If **Transfer Client IP Address** is enabled, a server cannot serve as both a backend server and a client.
This is because backend server will think the packet from the client is sent by itself and will not return a response packet to the load balancer. As a result, the return traffic will be interrupted.
- If **Transfer Client IP Address** is enabled, traffic, such as unidirectional data transmission or push traffic, may be interrupted when backend servers are being migrated. After backend servers are migrated, retransmit the packets to restore the traffic.
- If you add IP addresses as backend servers, the source IP addresses of the clients cannot be passed to these servers. Install the [TOA module](#) to obtain source IP addresses.

Alternatives for Obtaining the IP Address of a Client

You can obtain the IP address of a client in the ways listed in [Table 1-60](#).

Table 1-60 Alternatives

Listener Protocol	Alternatives
TCP	Configuring the TOA Module
HTTP/HTTPS/QUIC	Layer 7 Load Balancing
TLS	Table 1-22

1.8.2 TLS Security Policy

HTTPS encryption is commonly used for applications that require secure transmission of data, such as banks and finance. ELB allows you to use common TLS security policies to secure data transmission.

When you add HTTPS listeners, you can select the default security policies or create a custom policy to improve security.

A security policy is a combination of TLS protocols of different versions and supported cipher suites.

Default Security Policy

A later TLS version ensures higher HTTPS communication security, but is less compatible with some browsers.

You can use later TLS versions for applications that require enhanced security, and earlier TLS versions for applications that need wider compatibility.

Table 1-61 Default security policies

Security Policy	TLS Versions	Cipher Suites
TLS-1-0	TLS 1.2 TLS 1.1 TLS 1.0	<ul style="list-style-type: none"> ● ECDHE-RSA-AES256-GCM-SHA384 ● ECDHE-RSA-AES128-GCM-SHA256 ● ECDHE-ECDSA-AES256-GCM-SHA384 ● ECDHE-ECDSA-AES128-GCM-SHA256
TLS-1-1	TLS 1.2 TLS 1.1	<ul style="list-style-type: none"> ● AES128-GCM-SHA256 ● AES256-GCM-SHA384
TLS-1-2	TLS 1.2	<ul style="list-style-type: none"> ● 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

Security Policy	TLS Versions	Cipher Suites
tls-1-0-inherit	TLS 1.2 TLS 1.1 TLS 1.0	<ul style="list-style-type: none"> ● 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

Security Policy	TLS Versions	Cipher Suites
TLS-1-2-Strict	TLS 1.2	<ul style="list-style-type: none"> ● 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
TLS-1-0-WITH-1-3	TLS 1.3 TLS 1.2 TLS 1.1 TLS 1.0	<ul style="list-style-type: none"> ● 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_AES_128_GCM_SHA256 ● TLS_AES_256_GCM_SHA384 ● TLS_CHACHA20_POLY1305_SHA256 ● TLS_AES_128_CCM_SHA256 ● TLS_AES_128_CCM_8_SHA256

Security Policy	TLS Versions	Cipher Suites
TLS-1-2-FS-WITH-1-3	TLS 1.3 TLS 1.2	<ul style="list-style-type: none"> • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • 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
TLS-1-2-FS	TLS 1.2	<ul style="list-style-type: none"> • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384
tls-1-2-strict-no-cbc	TLS 1.2	<ul style="list-style-type: none"> • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256

 **NOTE**

The above table lists the cipher suites supported by ELB. Generally, clients also support multiple cipher suites. In actual use, the cipher suites supported by ELB and clients are used, and the cipher suites supported by ELB take precedence.

Differences Among Default Security Policies

√ indicates the metric is supported, and x indicates the metric is not supported.

Table 1-62 Differences between TLS security policies

Security Policy	tls-1-0	tls-1-1	tls-1-2	tls-1-0 - inherit	tls-1-2 - strict	tls-1-0-with-1-3	tls-1-2-fs-with-1-3	tls-1-2-fs	hybrid-policy-1-0	tls-1-2-strict-no-cbc
Protocol-TLS 1.3	x	x	x	x	x	√	√	√	x	x
Protocol-TLS 1.2	√	√	√	√	√	√	√	√	√	√
Protocol-TLS 1.1	√	√	x	√	x	√	x	x	√	x
Protocol-TLS 1.0	√	x	x	√	x	√	x	x	x	x

Table 1-63 Differences between TLS security policies (cipher suites)

Security Policy	tls-1-0	tls-1-1	tls-1-2	tls-1-0 - inherit	tls-1-2 - strict	tls-1-0-with-1-3	tls-1-2-fs-with-1-3	tls-1-2-fs	hybrid-policy-1-0	tls-1-2-strict-no-cbc
ECDHE-RSA-AES128-GCM-SHA256	√	√	√	x	√	x	x	x	x	√
ECDHE-RSA-AES256-GCM-SHA384	√	√	√	√	√	√	√	√	√	√
ECDHE-RSA-AES128-SHA256	√	√	√	√	√	√	√	√	√	x
ECDHE-RSA-AES256-SHA384	√	√	√	√	√	√	√	√	√	x
AES128-GCM-SHA256	√	√	√	√	√	√	x	x	√	x

Security Policy	tls-1-0	tls-1-1	tls-1-2	tls-1-0 - inherit	tls-1-2 - strict	tls-1-0-with-1-3	tls-1-2-fs-with-1-3	tls-1-2-fs	hybrid-policy-1-0	tls-1-2-strict-no-cbc
AES256-GCM-SHA384	√	√	√	√	√	√	×	×	√	×
AES128-SHA256	√	√	√	√	√	√	×	×	√	×
AES256-SHA256	√	√	√	√	√	√	×	×	√	×
ECDHE-RSA-AES128-SHA	√	√	√	√	×	√	×	×	√	×
ECDHE-RSA-AES256-SHA	√	√	√	√	×	√	×	×	√	×
AES128-SHA	√	√	√	√	×	√	×	×	√	×
AES256-SHA	√	√	√	√	×	√	×	×	√	×
ECDHE-ECDSA-AES128-GCM-SHA256	√	√	√	√	√	√	√	√	√	√
ECDHE-ECDSA-AES128-SHA256	√	√	√	√	√	√	√	√	√	×
ECDHE-ECDSA-AES128-SHA	√	√	√	√	×	√	×	×	√	×
ECDHE-ECDSA-AES256-GCM-SHA384	√	√	√	√	√	√	√	√	√	√
ECDHE-ECDSA-AES256-SHA384	√	√	√	√	√	√	√	√	√	×

Security Policy	tls-1-0	tls-1-1	tls-1-2	tls-1-0 - inherit	tls-1-2 - strict	tls-1-0-with-1-3	tls-1-2-fs-with-1-3	tls-1-2-fs	hybrid-policy-1-0	tls-1-2-strict-no-cbc
ECDHE-ECDSA-AES256-SHA	√	√	√	√	×	√	×	×	√	×
ECDHE-RSA-AES128-GCM-SHA256	×	×	×	√	×	√	√	√	√	×
TLS_AES_256_GCM_SHA384	×	×	×	×	×	√	√	√	×	×
TLS_CHACHA20_POLY1305_SHA256	×	×	×	×	×	√	√	√	×	×
TLS_AES_128_GCM_SHA256	×	×	×	×	×	√	√	√	×	×
TLS_AES_128_CCM_8_SHA256	×	×	×	×	×	√	√	√	×	×
TLS_AES_128_CCM_SHA256	×	×	×	×	×	√	√	√	×	×
DHE-RSA-AES128-SHA	×	×	×	√	×	×	×	×	×	×
DHE-DSS-AES128-SHA	×	×	×	√	×	×	×	×	×	×
CAMELLIA128-SHA	×	×	×	√	×	×	×	×	×	×
EDH-RSA-DES-CBC3-SHA	×	×	×	√	×	×	×	×	×	×
DES-CBC3-SHA	×	×	×	√	×	×	×	×	×	×
ECDHE-RSA-RC4-SHA	×	×	×	√	×	×	×	×	×	×

Security Policy	tls-1-0	tls-1-1	tls-1-2	tls-1-0 - inherit	tls-1-2 - strict	tls-1-0-with-1-3	tls-1-2-fs-with-1-3	tls-1-2-fs	hybrid-policy-1-0	tls-1-2-strict-no-cbc
RC4-SHA	x	x	x	√	x	x	x	x	x	x
DHE-RSA-AES256-SHA	x	x	x	√	x	x	x	x	x	x
DHE-DSS-AES256-SHA	x	x	x	√	x	x	x	x	x	x
DHE-RSA-CAMELLIA256-SHA	x	x	x	√	x	x	x	x	x	x
ECC-SM4-SM3	x	x	x	x	x	x	x	x	√	x
ECDHE-SM4-SM3	x	x	x	x	x	x	x	x	√	x

Table 1-64 Security policies and compatible browsers and clients

Security Policy	tls-1-0	tls-1-1	tls-1-2	tls-1-0 - inherit	tls-1-2 - strict	tls-1-0-with-1-3	tls-1-2-fs-with-1-3	tls-1-2-fs	hybrid-policy-1-0	tls-1-2-strict-no-cbc
Android 8.0	√	√	√	√	√	√	√	√	√	√
Android 9.0	√	√	√	√	√	√	√	√	√	√
Chrome 70 / Win 10	√	√	√	√	√	√	√	√	√	√
Chrome 80 / Win 10	√	√	√	√	√	√	√	√	√	√
Firefox 62 / Win 7	√	√	√	√	√	√	√	√	√	√
Firefox 73 / Win 10	√	√	√	√	√	√	√	√	√	√
IE 8 / XP	√	√	√	√	x	√	x	x	x	x

Security Policy	tls-1-0	tls-1-1	tls-1-2	tls-1-0 - inherit	tls-1-2 - strict	tls-1-0-with-1-3	tls-1-2-fs-with-1-3	tls-1-2-fs	hybrid-policy-1-0	tls-1-2-strict-no-cbc
IE 8-10 / Win 7	√	√	√	√	×	√	×	×	×	×
IE 11 / Win 7	√	√	√	√	√	√	√	√	√	√
IE 11 / Win 10	√	√	√	√	√	√	√	√	√	√
Edge 15 / Win 10	√	√	√	√	√	√	√	√	√	√
Edge 16 / Win 10	√	√	√	√	√	√	√	√	√	√
Edge 18 / Win 10	√	√	√	√	√	√	√	√	√	√
Java 8u161	√	√	√	√	√	√	√	√	√	√
Java 11.0.3	√	√	√	√	√	√	√	√	√	√
Java 12.0.1	√	√	√	√	√	√	√	√	√	√
OpenSSL 1.0.2s	√	√	√	√	√	√	√	√	√	√
OpenSSL 1.1.0k	√	√	√	√	√	√	√	√	√	√
OpenSSL 1.1.1c	√	√	√	√	√	√	√	√	√	√
Safari 10 / iOS 10	√	√	√	√	√	√	√	√	√	√
Safari 10 / OS X 10.12	√	√	√	√	√	√	√	√	√	√
Safari 12.1.1 / iOS 12.3.1	√	√	√	√	√	√	√	√	√	√

Creating a Custom Security Policy

ELB allows you to use common TLS security policies to secure data transmission. If you need to use a certain TLS version and disable some cipher suites, you can create a custom security policy and add it to an HTTPS listener to improve service security.

1. Go to the [load balancer list page](#).
2. In the navigation pane on the left, choose **TLS Security Policies**.
3. On the displayed page, click **Create Custom Security Policy** in the upper right corner.
4. Configure the parameters based on [Table 1-65](#).

Table 1-65 Custom security policy parameters

Parameter	Description
Name	Specifies the name of the custom security policy.
TLS Version	Specifies the TLS version supported by the custom security policy. You can select multiple versions: <ul style="list-style-type: none">• TLS 1.0• TLS 1.1• TLS 1.2• TLS 1.3
Cipher Suite	Specifies the cipher suites that match the selected TLS versions.
Description	Provides supplementary information about the custom security policy.

5. Click **OK**.

Managing a Custom Security Policy

After a custom security policy is created, you can modify or delete it.

Modifying a Custom Security Policy

You can modify the name, TLS version, cipher suite, and description of a custom security policy as required.

1. Go to the [load balancer list page](#).
2. In the navigation pane on the left, choose **TLS Security Policies**.
3. On the **TLS Security Policies** page, click **Custom Security Policies**, locate the custom security policy, and click **Modify** in the **Operation** column.
4. In displayed dialog box, modify the custom security policy as described in [Table 1-65](#).
5. Click **OK**.

Deleting a Custom Security Policy

You can delete a custom security policy as you need.

 **NOTE**

If a custom security policy is used by a listener, it cannot be deleted. Disassociate the security policy from the listener first.

1. Go to the [load balancer list page](#).
2. In the navigation pane on the left, choose **TLS Security Policies**.
3. On the **TLS Security Policies** page, click **Custom Security Policies**, locate the custom security policy, and click **Delete** in the **Operation** column.
4. In the displayed dialog box, click **OK**.

Selecting a Security Policy for an HTTPS Listener

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
3. Under **Listeners**, click **Add Listener**.
4. On the **Add Listener** page, set **Frontend Protocol** to **HTTPS**.
5. Expand **Advanced Settings** and select a security policy.
You can select a [default security policy](#) or a custom security policy.
If there is no custom security policy, you can create one by referring to [Creating a Custom Security Policy](#).
6. Confirm the configurations and go to the next step.

Changing a Security Policy for an HTTPS Listener

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
3. Click **Listeners**, locate the listener, and click its name.
4. On the **Summary** tab, click **Edit** on the top right.
5. In the **Edit** dialog box, expand **Advanced Settings** and change the security policy.
6. Click **OK**.

1.8.3 SNI Certificate

Server Name Indication (SNI) is an extension of the Transport Layer Security (TLS) protocol. It is used when a server uses multiple domain names and certificates.

Scenarios

If you have an application that can be accessed through multiple domain names and each domain name uses a different certificate, you can enable SNI when you add an HTTPS listener.

After SNI is enabled, you need to select SNI certificates based on the domain names. The client submits the requested domain name while sending an SSL handshake. Once receiving the request, the load balancer searches for the certificate based on the domain name. If the certificate is found, this certificate will be used for authentication. If no SNI certificates are found, the server certificate is used for authentication.

Notes and Constraints

- SNI can be only enabled for HTTPS and TLS listeners.
- After SNI is enabled, select an SNI certificate by referring to [Adding a Certificate](#).
- If a certificate has expired, you need to manually replace or delete it by following the instructions in [Binding or Replacing a Certificate](#).
- An HTTPS listener can have up to 30 SNI certificates. All the certificates can have up to 30 domain names.

NOTE

Listeners of a dedicated load balancer can have up to 50 SNI certificates. You can [submit a service ticket](#) to increase the quota.

Restrictions

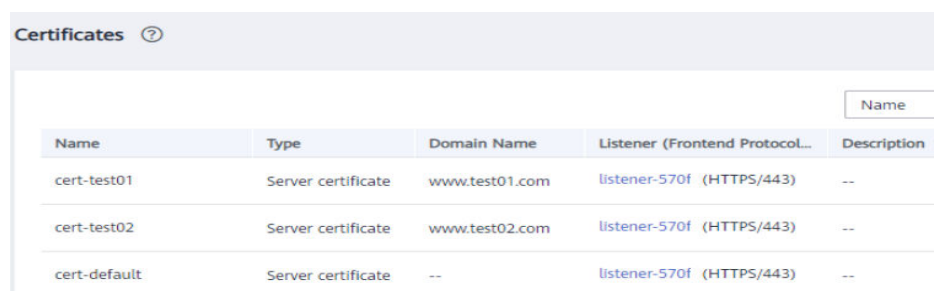
- You must specify at least one domain name for each SNI certificate. The domain name must be the same as that in the certificate.
- A domain name can be used by both an ECC certificate and an RSA certificate. If there are two SNI certificates that use the same domain name, the ECC certificate is displayed preferentially.

How SNI Certificates and Domain Names Are Matched

- Domain names in an SNI certificate are matched as follows:
If the domain name of the certificate is *.test.com, a.test.com and b.test.com are supported, but a.b.test.com and c.d.test.com are not supported.
The domain name with the longest suffix is matched. If a certificate contains both *.b.test.com and *.test.com, a.b.test.com preferentially matches *.b.test.com.
- **cert-default** is the default certificate bound to the HTTPS listener, and **cert-test01** and **cert-test02** are SNI certificates.
The domain name of **cert-test01** is **www.test01.com** and that of **cert-test02** is **www.test02.com**.

If the requested domain name matches either of the domain names, the corresponding SNI certificate will be used for authentication. If no domain name is matched, the default server certificate is used for authentication.

Figure 1-25 Configuring certificates

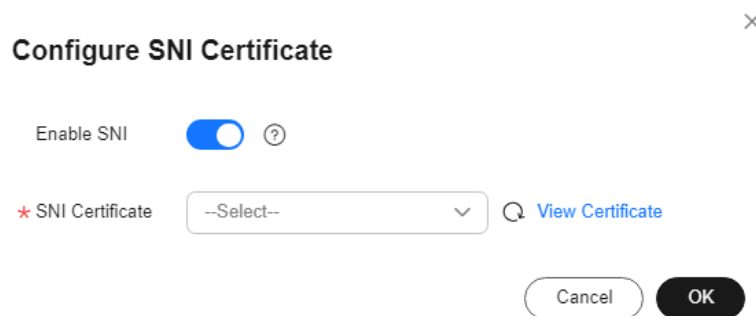


Name	Type	Domain Name	Listener (Frontend Protocol...)	Description
cert-test01	Server certificate	www.test01.com	listener-570f (HTTPS/443)	--
cert-test02	Server certificate	www.test02.com	listener-570f (HTTPS/443)	--
cert-default	Server certificate	--	listener-570f (HTTPS/443)	--

Enabling SNI for an HTTPS Listener

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
3. Click **Listeners**, locate the listener, and click its name.
4. On the **Summary** tab, click **Configure** on the right of SNI.
5. Enable SNI and select an SNI certificate.

Figure 1-26 Configuring an SNI certificate



6. Click **OK**.

1.8.4 Certificate

1.8.4.1 Certificate Overview

When you add an HTTPS or TLS listener, you need to bind a server certificate to it. To enable mutual authentication, you also need to bind a CA certificate to the listener. You can purchase a server certificate from Huawei Cloud Cloud Certificate Manager (CCM) or upload your own certificates to the ELB console.

Use Cases

When you add an HTTPS or TLS listener to route requests, you need to select **SSL Authentication**. For one-way authentication, you need to configure a server certificate for the listener. For two-way authentication, you need to configure both a server certificate and a CA certificate.

Table 1-66 SSL authentication

One-way Authentication	Only backend servers will be authenticated. You need to bind a server certificate to the listener to authenticate the server.
Mutual Authentication	The clients and the load balancer authenticate each other. Only authenticated clients will be allowed to access the load balancer. You need to bind both a server certificate and a CA certificate to the listener to allow the clients and the load balancer to authenticate each other. You do not need to configure two-way authentication on the backend servers.

ELB supports two types of certificates.

Table 1-67 Certificate types

Server Certificate	Used for SSL handshake negotiations if an HTTPS or TLS listener is used. Both the certificate content and private key are required.
CA Certificate	Also called client CA public key certificate and used to verify the client certificate issuer. If mutual authentication is required, connections can be established only when the client provides a certificate issued by a specific CA.

Precautions

- A certificate can be used by multiple load balancers but only needs to be uploaded to ELB once.
- You must specify a domain name for an SNI certificate. The domain name must be the same as that in the certificate. An SNI certificate can have multiple domain names.
- For each certificate type, a listener can have only one certificate by default, but a certificate can be bound to more than one listener. If SNI is enabled for the listener, multiple server certificates can be bound.
- Only original certificates are supported. That is to say, you cannot encrypt your certificates.
- You can use self-signed certificates. However, note that self-signed certificates pose security risks. It is recommended that you use certificates issued by third parties.
- ELB only supports certificates in PEM format. If you have a certificate in any other format, you must convert it to a PEM-encoded certificate.
- If a certificate has expired, you need to manually replace or delete it.

Certificate Format

You can copy and paste the certificate body to create a certificate or directly upload a certificate.

A certificate issued by the Root CA is unique, and no additional certificates are required. The configured site is considered trustable by access devices, such as a browser.

The body of the server and CA certificates must meet the requirements as described below.

- The content must start with -----BEGIN CERTIFICATE----- and ends with -----END CERTIFICATE-----.
- Each row contains 64 characters except the last row.

- There are no empty rows.

The following is an example:

```
-----BEGIN CERTIFICATE-----  
Base64-encoded certificate  
-----END CERTIFICATE-----
```

Private Key Format

When creating a server certificate, you also need to upload the private key of the certificate. You can copy and paste the private key content or directly upload the private key in the required format.

Private keys must be unencrypted and meet the following requirements:

- The value must be in PEM format.
 - The content must start with **-----BEGIN RSA PRIVATE KEY-----** and end with **-----END RSA PRIVATE KEY-----**.
 - The content must start with **-----BEGIN EC PRIVATE KEY-----** and end with **-----END EC PRIVATE KEY-----**.
- There are no empty rows. Each row contains 64 characters except the last row.

The following is an example:

```
-----BEGIN RSA PRIVATE KEY-----  
[key]  
-----END RSA PRIVATE KEY-----
```

Converting Certificate Formats

ELB only supports certificates in PEM format. If you have a certificate in any other format, you must convert it to a PEM-encoded certificate. There are some common methods for converting a certificate from any other format to PEM.

From DER to PEM

The DER format is usually used on a Java platform.

Run the following command to convert the certificate format:

```
openssl x509 -inform der -in certificate.cer -out certificate.pem
```

Run the following command to convert the private key format:

```
openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem
```

From P7B to PEM

The P7B format is usually used by Windows and Tomcat servers.

Run the following command to convert the certificate format:

```
openssl pkcs7 -print_certs -in incertificate.p7b -out outcertificate.cer
```

From PFX to PEM

The PFX format is usually used by Windows servers.

Run the following command to convert the certificate format:

```
openssl pkcs12 -in certname.pfx -nokeys -out cert.pem
```

Run the following command to convert the private key format:

```
openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes
```

1.8.4.2 Adding a Certificate

Scenarios

To enable authentication for securing data transmission over HTTPS, ELB allows you to bind the following certificates to HTTPS listeners of a load balancer:

- **Server certificate:** You can purchase a certificate from SSL Certificate Manager (SCM) or upload your own certificates.
- **CA certificate:** You can only upload your own CA certificates.
- **Server SM certificates:** You can purchase a certificate from SSL Certificate Manager (SCM) or upload your own certificates.

NOTE

If you want to use the same certificate in two regions, you need to add a certificate in each region.

Adding a Server Certificate

1. Go to the [load balancer list page](#).
2. In the navigation pane on the left, choose **Certificates**.
3. Click **Add Certificate** on the top right corner and set parameters by referring to [Table 1-68](#).

Table 1-68 Server certificate parameters

Parameter	Description
Certificate Type	Specifies the certificate type. Select Server certificate . <ul style="list-style-type: none">• Server certificate: used for SSL handshake negotiations if an HTTPS listener is used. Both the certificate content and private key are required.• CA certificate: issued by a certificate authority (CA) and used to verify the certificate issuer. If HTTPS mutual authentication is required, HTTPS connections can be established only when the client provides a certificate issued by a specific CA.

Parameter	Description
Source	<p>Specifies the source of a certificate. You can purchase a certificate from CCM or upload your own certificates.</p> <ul style="list-style-type: none"> • SSL Certificate Manager: server certificates provided by CCM. You need to buy a certificate or upload your own certificates. • Your certificate: You need to upload the certificate content and private key of your own certificate to the ELB console. <p>NOTE You are advised to use SCM to manage your certificates.</p>
Certificate	<p>This parameter is only available for certificates managed on the CCM console. You can select a certificate managed by CCM.</p>
Certificate Name	<p>Specifies the name of your certificate. This parameter is only available for your certificates.</p>
Enterprise Project	<p>Specifies an enterprise project by which cloud resources and members are centrally managed.</p>
Certificate Content	<p>Specifies the content of a certificate. This parameter is only available for your certificates. The content must be in PEM format. Click Upload and select the certificate to be uploaded. Ensure that your browser is of the latest version. The format of the certificate body is as follows: -----BEGIN CERTIFICATE----- Base64-encoded certificate -----END CERTIFICATE-----</p>
Private Key	<p>Specifies the private key of a certificate. This parameter is only available for your certificates. Click Upload and select the private key to be uploaded. Ensure that your browser is of the latest version. The value must be an unencrypted private key. The private key must be in PEM format as follows: -----BEGIN PRIVATE KEY----- [key] -----END PRIVATE KEY-----</p>

Parameter	Description
SNI Domain Name (Optional)	<p>The domain name must be specified if the certificate is intended for SNI.</p> <p>A domain name can contain only letters, digits, and hyphens (-) and consist of multiple labels (max. 63 characters each) separated by periods (.). It cannot start or end with a hyphen (-).</p> <p>You can specify up to 100 domain names, separated by commas (,). A domain name can contain a maximum of 100 characters, and the total length cannot exceed 10,000 characters.</p>
Description	(Optional) Provides supplementary information about the certificate.

4. Click **OK**.

Adding a CA Certificate

1. Go to the [load balancer list page](#).
2. In the navigation pane on the left, choose **Certificates**.
3. Click **Add Certificate** on the top right corner and set parameters by referring to [Table 1-69](#).

Table 1-69 CA certificate parameters

Parameter	Description
Certificate Type	<p>Specifies the certificate type. Select CA certificate.</p> <ul style="list-style-type: none">• Server certificate: used for SSL handshake negotiations if an HTTPS listener is used. Both the certificate content and private key are required.• CA certificate: issued by a certificate authority (CA) and used to verify the certificate issuer. If HTTPS mutual authentication is required, HTTPS connections can be established only when the client provides a certificate issued by a specific CA.
Certificate Name	Specifies the name of the CA certificate.
Enterprise Project	Specifies an enterprise project by which cloud resources and members are centrally managed.

Parameter	Description
Certificate Content	<p>Specifies the content of the CA certificate. The certificate must be a PEM file.</p> <p>Click Upload and select the certificate to be uploaded. Ensure that your browser is of the latest version.</p> <p>The format of the certificate body is as follows:</p> <pre>-----BEGIN CERTIFICATE----- Base64-encoded certificate -----END CERTIFICATE-----</pre>
Description	(Optional) Provides supplementary information about the certificate.

4. Click **OK**.

1.8.4.3 Managing Certificates

Scenarios

You can manage your certificates on the ELB console. If a certificate is no longer needed, you can delete it.

Notes and Constraints

A certificate that has been bound to an HTTPS listener cannot be deleted. Disassociate the certificate from the listener first by referring to [Replacing a Certificate](#).

Querying Listeners by Certificate

1. Go to the [load balancer list page](#).
2. In the navigation pane on the left, choose **Certificates**.
3. In the certificate list, click the listener name in the **Listener (Frontend Protocol/Port)** column to view its details.

If there are more than 5 listeners, no listener is displayed in the **Listener (Frontend Protocol/Port)** column. Click **View All**. On the displayed page, click **Listeners**, locate the listener, and click its name to view its details.

Modifying a Certificate

1. Go to the [load balancer list page](#).
2. In the navigation pane on the left, choose **Certificates**.
3. Locate the certificate and click **Modify** in the **Operation** column.
4. In the **Modify Certificate** dialog box, modify the parameters as required.
5. Confirm the information and click **OK**.

Deleting a Certificate

1. Go to the [load balancer list page](#).
2. In the navigation pane on the left, choose **Certificates**.
3. Locate the certificate and click **Delete** in the **Operation** column.
4. In the displayed dialog box, click **OK**.

1.8.4.4 Binding or Replacing a Certificate

Scenarios

You need to bind a certificate when you add an HTTPS listener to a load balancer. If the certificate used by a listener has expired or needs to be replaced due to other reasons, you can replace the certificate on the **Listeners** tab.

If the certificate is also used by other services such as WAF, replace the certificate on all these services to prevent service unavailability.

NOTE

Replacing a certificate and private keys does not affect your applications.

Notes and Constraints

- Only HTTPS listeners require certificates.
- If a certificate has expired, you need to manually replace or delete it.
- The new certificate takes effect immediately. The old certificate is used for established connections, and the new one is used for new connections.

Prerequisites

You have added a certificate by following the instructions in [Adding a Certificate](#).

Binding a Certificate

You can bind certificates when you add an HTTPS listener. For details, see [Adding an HTTPS Listener](#).

Replacing a Certificate

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
3. Click the **Listeners** tab, locate the listener, and click **Edit** in **Operation** column.
4. On the displayed dialog box, select a server certificate or CA certificate.
5. Click **OK** in the **Edit** dialog box.

1.8.4.5 Replacing the Certificate Bound to Different Listeners

Scenario

If the certificate that is bound to different listeners has expired or needs to be replaced due to other reasons, you can replace the certificate by modifying it on the **Certificates** page.

NOTE

Replacing the certificate and private keys does not affect your applications.

Notes and Constraints

- Only HTTPS and QUIC listeners require certificates.
- The new certificate takes effect immediately. The previous certificate is used for established connections, and the new one is used for new connections.
- SSL Certificate Manager (SCM) allows you to purchase a certificate from Huawei Cloud or upload your own certificates for easier management.

Modifying a Certificate

1. Go to the [load balancer list page](#).
2. In the navigation pane on the left, choose **Certificates**.
3. Locate the certificate and click **Modify** in the **Operation** column.
4. Modify the parameters as required.
5. Confirm the information and click **OK**.

1.8.5 Access Control

1.8.5.1 What Is Access Control?

Access control allows you to add a whitelist or blacklist to specify IP addresses that are allowed or denied to access a listener.

NOTE

Network ACL rules configured for the frontend subnet of a load balancer do not restrict traffic from clients to the load balancer. Use access control to limit which IP addresses can access the load balancer.

Whitelist and Blacklist

You can set a whitelist or blacklist to control access to a listener.

- Once the whitelist is set, only the IP addresses or CIDR blocks specified in the IP address group can access the listener.

Access control policies only take effect for new connections, but not for connections that have been established. If a whitelist is configured for a listener but IP addresses that are not in the whitelist can access the backend server associated with the listener, one possible reason is that a persistent connection is established between the client and the backend server. To deny

IP addresses that are not in the whitelist from accessing the listener, the persistent connection between the client and the backend server needs to be disconnected.

- Once the blacklist is set, the IP addresses or CIDR blocks specified in the blacklist cannot access the listener.

NOTE

- Access control does not restrict the ping command. You can still ping a load balancer from restricted IP addresses.
- Whitelists and blacklists do not conflict with inbound security group rules. Access control defines the IP addresses or CIDR blocks that are allowed or denied to access listeners, while inbound security group rules control access to backend servers. Requests first match the access control policy then the security group rules before they finally reach backend servers.

Configuring Access Control

NOTICE

Note that modifying an access control policy may interrupt your services or cause network security risks.

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
3. Configure access control for a listener in either of the following ways:
 - On the **Listeners** page, locate the listener and click **Configure** in the **Access Control** column.
 - Click the name of the target listener. On the **Summary** page, click **Configure** on the right of **Access Control**.
4. In the displayed **Configure Access Control** dialog box, configure parameters as described in [Table 1-70](#).

Table 1-70 Parameter description

Parameter	Description
Access Control	Specifies how access to the listener is controlled. Three options are available: <ul style="list-style-type: none">• All IP addresses: All IP addresses can access the listener.• Whitelist: Only IP addresses in the IP address group can access the listener.• Blacklist: IP addresses in the IP address group are not allowed to access the listener.

Parameter	Description
IP Address Group	Specifies the IP address group associated with a whitelist or blacklist. If there is no IP address group, create one first. For more information, see What Is an IP Address Group? A maximum of five IP address groups can be selected.
Access Control	If you have set Access Control to Whitelist or Blacklist , you can enable or disable access control. <ul style="list-style-type: none">• Only after you enable access control, the whitelist or blacklist takes effect.• If you disable access control, the whitelist or blacklist does not take effect.

5. Click **OK**.

1.8.5.2 IP Address Group

What Is an IP Address Group?

An IP address group allows you to manage a collection of IP addresses that have the same security requirements or whose security requirements change frequently.

If you want to use a whitelist or blacklist for **access control**, you must select an IP address group. For details, see [What Is Access Control?](#)

- **Whitelist:** Only IP addresses in the IP address group can access the listener. If the IP address group does not contain any IP address and you have selected a whitelist for access control, no IP addresses can access the listener.
- **Blacklist:** IP addresses in the IP address group are denied to access the listener. If the IP address group does not contain any IP address and you have selected a blacklist for access control, all IP addresses can access the listener.

Notes and Constraints

- By default, you can create a maximum of 50 IP address groups.
- An IP address group can be associated with a maximum of 50 listeners.

Creating an IP Address Group

1. Go to the [load balancer list page](#).
2. In the navigation pane on the left, choose **Elastic Load Balance > IP Address Groups**.
3. On the displayed page, click **Create IP Address Group**.
4. Configure the parameters based on [Table 1-71](#).

Table 1-71 IP address group parameters

Parameter	Description	Example Value
Name	Specifies the name of the IP address group.	ipGroup-01
Enterprise Project	Specifies an enterprise project by which cloud resources and members are centrally managed. For details, see the Enterprise Management User Guide .	N/A
IP Addresses	Specifies IPv4 or IPv6 IP addresses or CIDR blocks that are added to the whitelist or blacklist for access control. <ul style="list-style-type: none">Each line contains a single IP address, a CIDR block, or an IP address range, and ends with a line break.You can add remarks at the end of each IP address or CIDR block and separate them with a vertical bar (). The remarks can be up to 255 characters long. Angle brackets (<>) are not allowed.You can add a maximum of 300 IP addresses or CIDR blocks to each IP address group.	<ul style="list-style-type: none">Without remarks: 10.168.2.24With remarks: 10.168.16.0/24 ECS01
Description	Provides supplementary information about the IP address group.	N/A

5. Click **OK**.

Managing IP Addresses in an IP Address Group

After an IP address group is created, you can manage the IP addresses in an IP address group as required:

- [Adding IP Addresses](#)
- [Changing IP Addresses](#)
- [Deleting an IP Address](#)

The IP addresses can be in the formats as described in [Table 1-71](#).

Adding IP Addresses

You can add IP addresses to an existing IP address group.

1. Go to the [load balancer list page](#).
2. In the navigation pane on the left, choose **Elastic Load Balance > IP Address Groups**.
3. On the **IP Address Groups** page, locate the target IP address group and click its name.
4. In the lower part of the displayed page, choose **IP Addresses** tab and click **Add IP Addresses**. On the **Add IP Addresses** page, add IP addresses.
5. Click **OK**.

Changing IP Addresses

You can perform the following steps to change all IP addresses in an IP address group:

1. Go to the [load balancer list page](#).
2. In the navigation pane on the left, choose **Elastic Load Balance > IP Address Groups**.
3. On the **IP Address Groups** page, you can:
 - a. Modify the basic information and change IP addresses of an IP address group:
 - i. Locate the target address group, click **Modify** in the **Operation** column. You can modify the name and description of an IP address group, and change all its IP addresses.
 - ii. Click **OK**.
 - b. Only change IP addresses:
 - i. Locate the target IP address group and click its name.
 - ii. In the lower part of the displayed page, choose **IP Addresses** tab, click **Change IP Address**, and change IP addresses as you need.
 - iii. Click **OK**.

Deleting an IP Address

If you want to delete IP addresses in batches from an IP address group, see [Changing IP Addresses](#).

To delete an IP address from an IP address group, perform the following operations:

1. Go to the [load balancer list page](#).
2. In the navigation pane on the left, choose **Elastic Load Balance > IP Address Groups**.
3. On the **IP Address Groups** page, locate the target IP address group and click its name.
4. In the IP address list, locate the IP address you want to delete and click **Delete** in the **Operation** column.
5. Confirm the information and click **OK**.

Viewing the Details of an IP Address Group

You can view the details of an IP address group, including:

- Name, ID, and creation time
 - IP addresses and CIDR blocks
 - Associated listeners
1. Go to the [load balancer list page](#).
 2. In the navigation pane on the left, choose **Elastic Load Balance > IP Address Groups**.
 3. On the **IP Address Groups** page, locate the target IP address group and click its name.
 4. Viewing the basic information about the IP address group.
 - a. On the **IP Addresses** tab, view the IP addresses or CIDR blocks.
 - b. On the **Associated Listeners** tab, view the listeners associated with the IP address group.

Deleting an IP Address Group

If an IP address group is used for controlling access to a listener, it cannot be deleted.

You can view the listeners associated with an IP address group by referring to [Viewing the Details of an IP Address Group](#). For details about how to disassociate an IP address group from a listener, see [Configuring Access Control](#).

1. Go to the [load balancer list page](#).
2. In the navigation pane on the left, choose **Elastic Load Balance > IP Address Groups**.
3. On the **IP Address Groups** page, locate the IP address group and click **Delete** in the **Operation** column.
4. Click **OK**.

1.8.6 Protection for Mission-Critical Operations

Scenarios

ELB supports sensitive operation protection. When you perform sensitive operations on the management console, you need to enter a credential that can prove your identity. You can perform corresponding operations only after your identity is authenticated. It is recommended that you enable operation protection to secure your account.

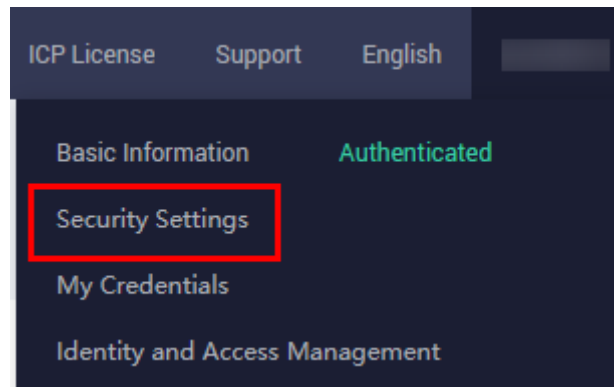
This function can be configured only by the administrator and takes effect for the resources in your account and the resources of users under your account. Common users have only the view permissions. To modify the permissions, contact the administrator.

Enabling Operation Protection

Operation protection is disabled by default. Perform the following operations to enable it:

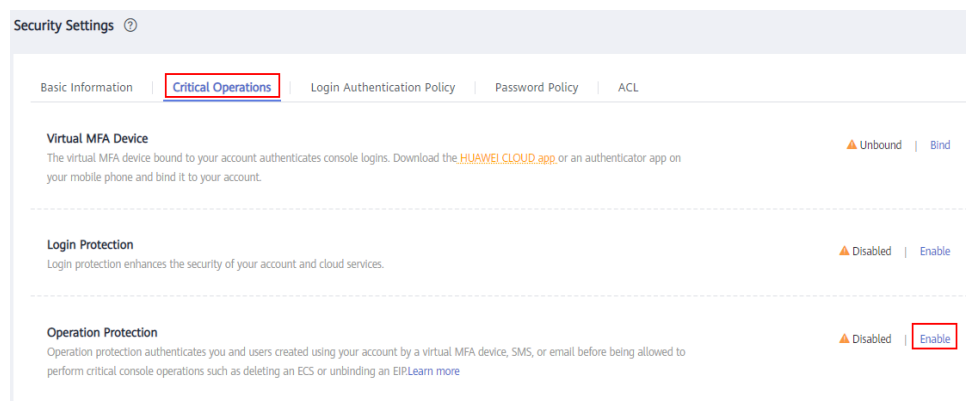
1. Log in to the management console.
2. Move the cursor to the username in the upper right corner of the page and select **Security Settings** from the list.

Figure 1-27 Security settings



3. On the **Security Settings** page, choose **Critical Operations > Operation Protection > Enable**.

Figure 1-28 Critical operations



4. On the **Operation Protection** page, select **Enable**.
If operation protection is enabled, you and IAM users created using your account need to enter a verification code when performing a critical operation, such as deleting an ECS resource.

NOTE

- When performing a critical operation, you will be asked to choose a verification method from email, SMS, and virtual MFA device.
 - If you have bound only a mobile number, only SMS verification is available.
 - If you have bound only an email address, only email verification is available.
 - If you have not bound an email address, mobile number, or virtual MFA device, bind one to perform critical operations.
- You can change the mobile number, email address, and virtual MFA device on the [Basic Information](#) page.

Verifying Operation Protection

After operation protection is enabled, when you perform a mission-critical operation, the system will verify your identity.

- If you have bound an email address, enter the email verification code.
- If you have bound a mobile number, enter the SMS verification code.
- If you have bound a virtual MFA device, enter a 6-digit dynamic verification code of the MFA device.

When you attempt to delete a load balancer, the following dialog box is displayed, and you need to select a verification method:

Figure 1-29 Identity verification

Identity Verification ×

i You have enabled operation protection. If you do not require operation protection for critical operations, go to Security Settings > Critical Operations > Operation Protection to disable it. [Disable Identity Verification](#)

Verification Method SMS Email Virtual MFA device ?

Mobile Number [Change](#)

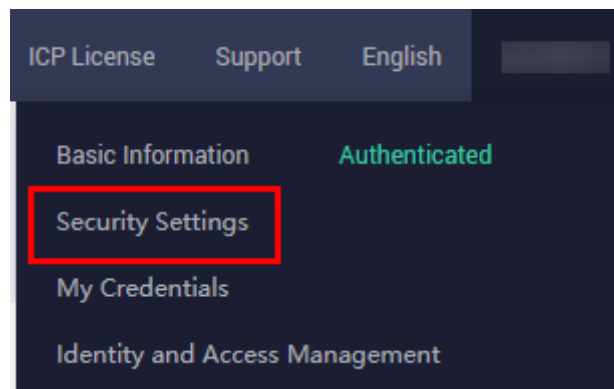
Verification Code

Disabling Operation Protection

Perform the following operations to disable operation protection:

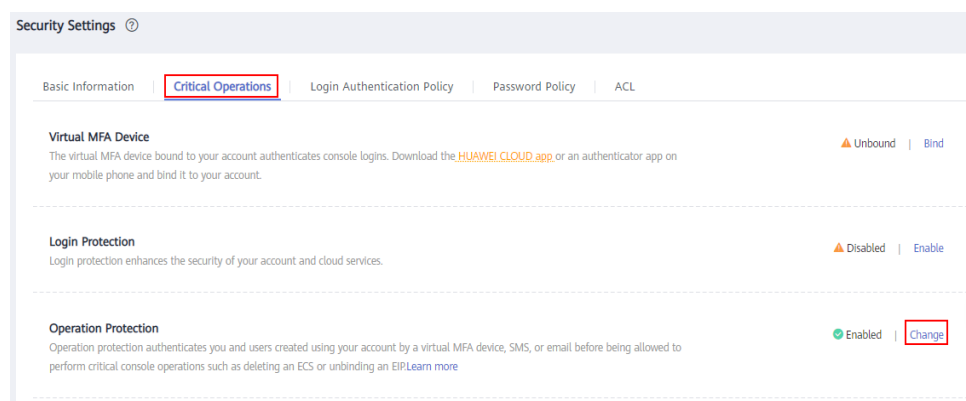
1. Log in to the management console.
2. Move the cursor to the username in the upper right corner of the page and select **Security Settings** from the list.

Figure 1-30 Security settings



3. On the **Security Settings** page, choose **Critical Operations** > **Operation Protection** > **Change**.

Figure 1-31 Modifying operation protection settings



4. On the **Operation Protection** page, select **Disable** and click **OK**.

References

- [How Do I Bind a Virtual MFA Device?](#)
- [How Do I Obtain an MFA Verification Code?](#)

1.9 Access Logging

Scenarios

ELB logs HTTP, HTTPS, and TLS requests received by load balancers, including the time when the request was sent, client IP address, request path, and server response.

With Log Tank Service (LTS), you can view logs of requests to load balancers at Layer 7 and analyze response status codes to quickly locate unhealthy backend servers.

 NOTE

ELB displays operations data, such as access logs, on the LTS console. Do not transmit private or sensitive data through fields in access logs. Encrypt your sensitive data if necessary.

Notes and Constraints

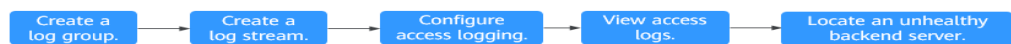
- Access logging can be configured only for load balancers that have HTTP QUIC, TLS, or HTTPS listeners.
- The access logs do not contain requests whose return code is **400 Bad Request**. This is because such requests do not comply with HTTP specification and cannot be processed properly.

Prerequisites

- You have created a load balancer that supports HTTP QUIC, TLS, or HTTPS. For details, see [Creating a Dedicated Load Balancer](#).
- You have enabled LTS. For details, see [Accessing LTS](#).
- You have created a backend server group, added backend servers to the group, and deployed services on the backend servers. For details, see [Creating a Backend Server Group](#).
- You have added an HTTP QUIC, TLS, or HTTPS listener to the load balancer.

Flowchart

Figure 1-32 Process for locating an unhealthy backend server



Creating a Log Group



1. Log in to the management console.
2. In the upper left corner of the page, click  and select the desired region and project.
3. Click  in the upper left corner and choose **Management & Governance > Log Tank Service**.
4. In the navigation pane on the left, choose **Log Management**.
5. On the lower part of the displayed page, click **Create Log Group**. In the displayed dialog box, enter a name for the log group.

Figure 1-33 Creating a log group

6. Confirm the settings and click **OK**.

Creating a Log Stream


1. On the LTS console, click  on the left of the target log group.
2. Click **Create Log Stream**. In the displayed dialog box, enter a name for the log stream.

Figure 1-34 Creating a log stream

3. Confirm the settings and click **OK**.

Configuring Access Logging


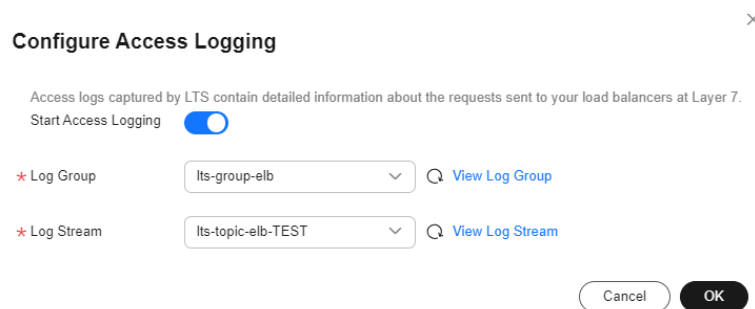
1. Click  in the upper left corner to display **Service List** and choose **Networking > Elastic Load Balance**.
2. On the **Load Balancers** page, locate the load balancer and click its name.
3. Under **Access Logs**, click **Configure Access Logging**.
4. Enable access logging and select the log group and log stream you have created.

Figure 1-35 Configuring access logging



5. Click **OK**.

NOTICE

Ensure that the log group is in the same region as the load balancer.

Viewing Access Logs

You can view details about access logs on the:

- ELB console: Click the name of the load balancer and click **Access Logs** to view logs.
- (Recommended) LTS console: Locate the target log group and click its name. On the displayed page, locate the target log stream and click **Real-Time Logs** tab.

The log format is as follows, which cannot be modified:

```
$msec $access_log_topic_id [$time_iso8601] $log_ver $remote_addr:$remote_port $status
"$request_method $scheme://$host$routier_request_uri $server_protocol" $request_length $bytes_sent
$body_bytes_sent $request_time "$upstream_status" "$upstream_connect_time" "$upstream_header_time"
"$upstream_response_time" "$upstream_addr" "$http_user_agent" "$http_referer" "$http_x_forwarded_for"
$lb_name $listener_name $listener_id
$pool_name "$member_name" $tenant_id $eip_address:$eip_port "$upstream_addr_priv" $certificate_id
$ssl_protocol $ssl_cipher $sni_domain_name $tcpinfo_rtt $self_defined_header
```

The following is a log example:

```
1644819836.370 eb11c5a9-93a7-4c48-80fc-03f61f638595 [2024-02-14T14:23:56+08:00] elb_01
192.168.1.1:888 200 "POST https://www.test.com/example/ HTTP/1.1" 1411 251 3 0.011 "200" "0.000"
"0.011" "0.011" "192.168.1.2:8080" "okhttp/3.13.1" "-" "-"
loadbalancer_295a7eee-9999-46ed-9fad-32a62ff0a687 listener_20679192-8888-4e62-a814-a2f870f62148
3333fd44fe3b42cbaa1dc2c641994d90 pool_89547549-6666-446e-9dbc-e3a551034c46 "-"
```

```
f2bc165ad9b4483a9b17762da851bbbb 121.64.212.1:443 "10.1.1.2:8080" - TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384 www.test.com 56704 -
```

Table 1-72 describes the fields in the log.

Table 1-72 Parameter description

Parameter	Description	Value Description	Example Value
msec	Time when the log is written, in seconds with a milliseconds resolution.	Floating-point data	1644819836.370
access_log_topic_id	Log stream ID.	uuid	eb11c5a9-93a7-4c48-80fc-03f61f638595
time_iso8601	Local time in the ISO 8601 standard format.	N/A	[2024-02-14T14:23:56+08:00]
log_ver	Log format version.	Fixed value: elb_01	elb_01
remote_addr: remote_port	IP address and port number of the client.	Records the IP address and port of the client.	192.168.1.1:888
status	HTTP status code.	Records the request status code.	200

Parameter	Description	Value Description	Example Value
request_method scheme://host request_uri server_protocol	<i>Request method Protocol://Host name: Request URI Request protocol</i>	<ul style="list-style-type: none"> ● request_method: request method ● scheme: HTTP or HTTPS ● host: host name, which can be a domain name or an IP address ● request_uri: indicates the native URI initiated by the browser without any modification and it does not include the protocol and host name. 	"POST https://www.test.com/example/ HTTP/1.1"
request_length	Length of the request received from the client, including the header and body.	Integer	1411
bytes_sent	Number of bytes sent to the client.	Integer	251
body_bytes_sent	Number of bytes sent to the client (excluding the response header).	Integer	3
request_time	Request processing time in seconds from the time when the load balancer receives the first request packet from the client to the time when the load balancer sends the response packet.	Floating-point data	0.011

Parameter	Description	Value Description	Example Value
upstream_status	<p>Response status code returned by the backend server.</p> <ul style="list-style-type: none">• When the load balancer attempts to retry a request, there will be multiple response status codes.• If the request is not correctly routed to the backend server, a hyphen (-) is displayed as a null value for this field.	HTTP status code returned by the backend server to the load balancer	"200"
upstream_connect_time	<p>Time taken to establish a connection with the server, in seconds, with a milliseconds resolution.</p> <ul style="list-style-type: none">• When the load balancer attempts to retry a request, there will be multiple connection times.• If the request is not correctly routed to the backend server, a hyphen (-) is displayed as a null value for this field.	Floating-point data	"0.000"

Parameter	Description	Value Description	Example Value
upstream_header_time	<p>Time taken to receive the response header from the server, in seconds, with a milliseconds resolution.</p> <ul style="list-style-type: none">• When the load balancer attempts to retry a request, there will be multiple response times.• If the request is not correctly routed to the backend server, a hyphen (-) is displayed as a null value for this field.	Floating-point data	"0.011"
upstream_response_time	<p>Time taken to receive the response from the server, in seconds, with a milliseconds resolution.</p> <ul style="list-style-type: none">• When the load balancer attempts to retry a request, there will be multiple response times.• If the request is not correctly routed to the backend server, a hyphen (-) is displayed as a null value for this field.	Floating-point data	"0.011"

Parameter	Description	Value Description	Example Value
upstream_addr	IP address and port number of the backend server. There may be multiple values separated by commas and spaces, and each value is in the format of <i>{IP address}:{Port number}</i> or <i>-</i> .	IP address and port number	"192.168.1.2:8080"
http_user_agent	http_user_agent in the request header received by the load balancer, indicating the system model and browser information of the client.	Records the browser-related information.	"okhttp/3.13.1"
http_referer	http_referer in the request header received by the load balancer, indicating the page link of the request.	Request for a page link	"-"
http_x_forwarded_for	http_x_forwarded_for in the request header received by the load balancer, indicating the IP address of the proxy server that the request passes through.	IP address	"-"
lb_name	Load balancer name in the format of loadbalancer_load balancer ID	String	loadbalancer_295a7eee-9999-46ed-9fad-32a62ffa687
listener_name	Listener name in the format of listener_listener ID .	String	listener_20679192-8888-4e62-a814-a2f870f62148

Parameter	Description	Value Description	Example Value
listener_id	Listener ID. This field can be ignored.	String	3333fd44fe3b42cbaa1dc2c641994d90
pool_name	Backend server group name in the format of pool_backend server group ID or pool_backend server group ID*load balancer ID .	String	pool_89547549-6666-446e-9dbc-e3a551034c46
member_name	Backend server name in the format of member_server ID . This field is not supported yet. There may be multiple values separated by commas and spaces, and each value is a member ID (member_id) or -.	String	"-"
tenant_id	Tenant ID.	String	f2bc165ad9b4483a9b17762da851bbbb
eip_address:eip_port	EIP of the load balancer and frontend port that were set when the listener was added.	EIP of the load balancer and frontend port that were set when the listener was added.	121.64.212.1:443
upstream_address:port	IP address and port number of the backend server. There may be multiple values separated by commas and spaces, and each value is in the format of {IP address}:{Port number} or -.	IP address and port number	"-" (Dedicated load balancers)

Parameter	Description	Value Description	Example Value
certificate_id	[HTTPS listener] Certificate ID used for establishing an SSL connection. This field is not supported yet.	String	N/A
ssl_protocol	[HTTPS listener] Protocol used for establishing an SSL connection. For a non-HTTPS listener, a hyphen (-) is displayed as a null value for this field.	String	TLSv1.2
ssl_cipher	[HTTPS listener] Cipher suite used for establishing an SSL connection. For a non-HTTPS listener, a hyphen (-) is displayed as a null value for this field.	String	ECDHE-RSA-AES256-GCM-SHA384
sni_domain_name	[HTTPS listener] SNI domain name provided by the client during SSL handshakes. For a non-HTTPS listener, a hyphen (-) is displayed as a null value for this field.	String	www.test.com
tcpinfo_rtt	TCP Round Trip Time (RTT) between the load balancer and client in microseconds.	Integer	56704
self_defined_header	This field is reserved. The default value is -.	String	N/A

Log analysis

At 14:23:56 GMT+08:00 on Feb 14, 2024, the load balancer receives an HTTP/1.1 POST request from a client whose IP address and port number are 192.168.1.1 and

888, then routes the request to a backend server whose IP address and port number are 100.64.0.129 and 8080, and finally returns 200 OK to the client after receiving the status code from the backend server.

Analysis results

The backend server responds to the request normally.

Locating an Unhealthy Backend Server

The following is a log that records an exception:

```
1554944564.344 - [2024-04-11T09:02:44+08:00] elb 10.133.251.171:51527 500 "GET http://10.154.73.58/
lrange/guestbook HTTP/1.1" 411 3726 3545 19.028 "500" "0.009" "19.028" "19.028" "172.17.0.82:3000"
"Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
73.0.3683.103 Safari/537.36" "http://10.154.73.58:5971/" "-" loadbalancer_ed0f790b-
e194-4657-9f97-53426227099e listener_b21dd0a9-690a-4945-950e-b134095c6bdd9
6b6aaf84d72b40fcb2d2b9b28f6a0b83
```

Log analysis

At 09:02:44 GMT+08:00 of April 11, 2024, the load balancer received a GET/HTTP/1.1 request from the client whose IP address and port number are 10.133.251.171 and 51527 respectively and then routed the request to a backend server that uses 172.17.0.82 and port 3000 to receive requests. The load balancer then received 500 Internal Server Error from the backend server and returned the status code to the client.

Analysis results

The backend server was unhealthy and failed to respond to the request.

NOTE

172.17.0.82:3000 is the private IP address of the backend server.

Configuring Log Transfer

If you want to analyze access logs later, transfer the logs to OBS or Data Ingestion Service (DIS) for storage.



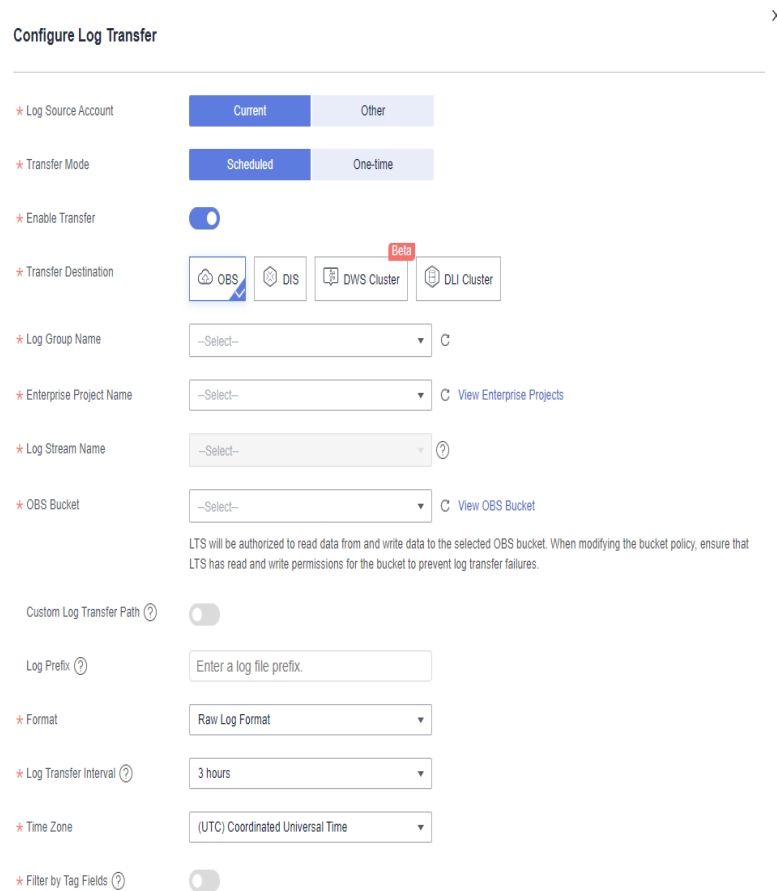
1. Log in to the management console.
2. In the upper left corner of the page, click  and select the desired region and project.
3. Click  in the upper left corner and **Management & Governance > Log Tank Service**.
4. In the navigation pane on the left, choose **Log Transfer**.
5. On the **Log Transfer** page, click **Configure Log Transfer** in the upper right corner.





Figure 1-36 Configuring log transfer

Configure Log Transfer X

* Log Source Account Current Other

* Transfer Mode Scheduled One-time

* Enable Transfer

* Transfer Destination  OBS  DIS  DWS Cluster Beta  DLI Cluster

* Log Group Name --Select-- C

* Enterprise Project Name --Select-- C [View Enterprise Projects](#)

* Log Stream Name --Select-- ?

* OBS Bucket --Select-- C [View OBS Bucket](#)

LTS will be authorized to read data from and write data to the selected OBS bucket. When modifying the bucket policy, ensure that LTS has read and write permissions for the bucket to prevent log transfer failures.

Custom Log Transfer Path ?

Log Prefix ?

* Format Raw Log Format

* Log Transfer Interval 3 hours

* Time Zone (UTC) Coordinated Universal Time

* Filter by Tag Fields ?

6. Configure the parameters. For details, see the [Log Tank Service User Guide](#).

1.10 Tags and Quotas

1.10.1 Tag



Scenarios

If you have a large number of cloud resources, you can add different tags to the resources to quickly identify them and use these tags to easily manage your resources.

Adding a Tag to a Load Balancer

You can add a tag to a load balancer in the following methods:

- Add a tag when you create a load balancer.
For details, see [Creating a Dedicated Load Balancer](#).
- Add a tag to an existing load balancer.
 - a. Log in to the management console.



- b. In the upper left corner of the page, click  and select the desired region and project.
- c. Click  in the upper left corner to display **Service List** and choose **Networking > Elastic Load Balance**.
- d. On the **Load Balancers** page, locate the load balancer and click its name.
- e. Under **Tags**, click **Add Tag**.
Each tag is a key-value pair, and the tag key is unique.
- f. In the **Add Tag** dialog box, enter a tag key and value and click **OK**.

 **NOTE**

A maximum of 20 tags can be added to a load balancer.

Adding a Tag to a Listener



To add a tag to an existing listener, perform the following steps:

1. Log in to the management console.
2. In the upper left corner of the page, click  and select the desired region and project.
3. Click  in the upper left corner to display **Service List** and choose **Networking > Elastic Load Balance**.
4. On the **Load Balancers** page, locate the load balancer and click its name.
5. Click **Listeners**, locate the listener, and click its name.
6. Under **Tags**, click **Add Tag**.
Each tag is a key-value pair, and the tag key is unique.
7. In the **Add Tag** dialog box, enter a tag key and value and click **OK**.

 **NOTE**

A maximum of 20 tags can be added to a listener.

Modifying a Tag

1. Log in to the management console.
2. In the upper left corner of the page, click  and select the desired region and project.
3. Click  in the upper left corner to display **Service List** and choose **Networking > Elastic Load Balance**.
4. On the **Load Balancers** page, locate the load balancer and click its name.
5. Click **Tags**, select the tag to be edited, and click **Edit** in the **Operation** column. In the **Edit Tag** dialog box, enter a tag value.



 **NOTE**

The tag key cannot be modified.

6. Click **OK**.

The operations for modifying a listener tag are not detailed here. Refer to the operations of modifying a load balancer tag.

Deleting a Tag

1. Log in to the management console.
2. In the upper left corner of the page, click  and select the desired region and project.
3. Click  in the upper left corner to display **Service List** and choose **Networking > Elastic Load Balance**.
4. On the **Load Balancers** page, locate the load balancer and click its name.
5. Click **Tags**, select the tag to be deleted, and click **Delete** in the **Operation** column.
6. In the displayed dialog box, click **OK**.

The operations for deleting a listener tag are not detailed here. Refer to the operations of deleting a load balancer tag.

1.10.2 Quotas

What Is Quota?

Quotas can limit the number of resources available to users, such as the maximum number of ECSs or EVS disks that can be created.

If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

How Do I View My Quotas?


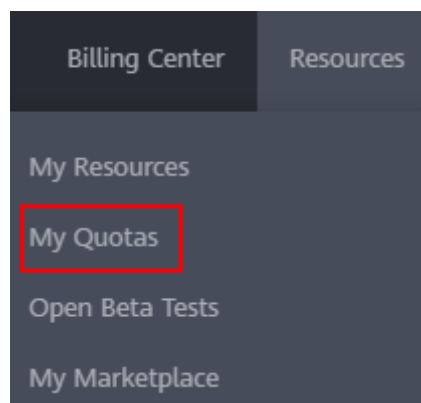
1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, choose **Resources > My Quotas**.
The **Service Quota** page is displayed.

Figure 1-37 My Quotas

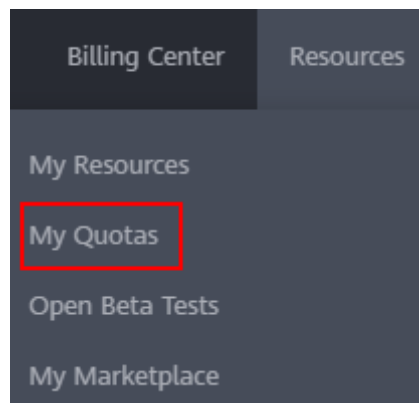


4. View the used and total quota of each type of resources on the displayed page.
If a quota cannot meet service requirements, apply for a higher quota.

How Do I Apply for a Higher Quota?

1. Log in to the management console.
2. In the upper right corner of the page, choose **Resources > My Quotas**.
The **Quotas** page is displayed.

Figure 1-38 My quotas



3. Click **Increase Quota** in the upper right corner of the page.

Figure 1-39 Increasing quota

Service	Resource Type	Used Quota	Total Quota
Auto Scaling	AS group	0	
	AS configuration	0	
Image Management Service	Image	0	
	Cluster	0	
Cloud Container Engine	Function	0	
	Code storage(MB)	0	
FunctionGraph	Disk	3	
	Disk capacity(GB)	120	
Elastic Volume Service	Snapshots	4	
	Protection group	0	
Storage Disaster Recovery Service	Replication pair	0	
	Backup Capacity(GB)	0	
Cloud Server Backup Service	Backup	0	
	File system	0	
Scalable File Service	File system capacity(GB)	0	
	Domain name	0	
CDN	File URL refreshing	0	
	Directory URL refreshing	0	
	URL refreshing	0	

4. On the **Create Service Ticket** page, configure parameters as required.
In the **Problem Description** area, fill in the content and reason for adjustment.
5. After all necessary parameters are configured, select **I have read and agree to the Ticket Service Protocol and Privacy Statement** and click **Submit**.

1.11 Cloud Eye Monitoring

1.11.1 Monitoring ELB Resources

Scenarios

Cloud Eye is a multi-dimensional resource monitoring service. You can use Cloud Eye to monitor ELB resources in real time, set alarm rules, identify resource exceptions, and quickly respond to resource changes.

Cloud Eye is enabled automatically after you create a load balancer. For more information about Cloud Eye, see [What Is Cloud Eye?](#)

Setting an Alarm Rule

You can set alarm rules on the Cloud Eye console to send you notifications in case of exceptions.

For details about how to set alarm rules, see [Creating an Alarm Rule](#).

On Cloud Eye, you can configure alarm rules for events. When there are specified events, you will receive alarm notifications. For details about how to create an alarm rule for an event, see [Creating an Alarm Rule to Monitor an Event](#).

Viewing Monitoring Metrics


You can view the metrics described in [ELB Monitoring Metrics](#) either on the ELB console or on the Cloud Eye console.


Viewing Monitoring Metrics on the ELB Console

1. Go to the [load balancer list page](#).
2. On the load balancer list page, locate the load balancer and click its name.
3. You can view metrics by load balancer, listener, and backend server group.
 - a. Load balancer: Click the **Monitoring** tab and select **Load balancer** for **Dimension**.
 - b. Listener (two ways):
 - i. Click the **Monitoring** tab, select **Listener** for **Dimension**, select the target listener, and view the monitoring metrics.
 - ii. Click the **Listeners** tab, locate the target listener, and click its name. Switch to the **Monitoring** tab and view the monitoring metrics.
 - c. Backend server group: Click the **Monitoring** tab and select **Backend server group** for **Dimension**.

Viewing Monitoring Metrics on the Cloud Eye Console

For details about how to view load balancer monitoring metrics on the Cloud Eye console, see [Querying Metrics of a Cloud Service](#).

1. Log in to the management console.
2. In the upper left corner of the page, click  and select the desired region and project.

3. Click  in the upper left corner and choose **Management & Governance > Cloud Eye**.
4. In the navigation pane on the left, choose **Cloud Service Monitoring**. In the displayed page, locate the **Dashboard** column and click **Elastic Load Balance ELB**.
5. On the displayed page, locate the target load balancer and click its name. Alternatively, locate the load balancer and click **View Metric** in the **Operation** column.
6. Select the time period during which you want to view metrics. You can select a system-defined time period (for example, last 1 hour) or specify a time period.
7. Click **Select Metric** in the upper right corner and select the metrics to be viewed.

Viewing Events

Cloud Eye monitors **ELB events** in real time. You can view the monitoring data on the Cloud Eye console.

For details about how to view the events, see [Viewing Event Monitoring Data](#).

1.11.2 ELB Monitoring Metrics

Overview

This section describes the namespace, the metrics that can be monitored by Cloud Eye, and dimensions of these metrics. You can view the [metrics reported by ELB and the generated alarms](#) on the Cloud Eye console.

Namespace

SYS.ELB

Load Balancer Metrics

For dedicated load balancers, you can view the monitoring metrics by load balancer, listener, backend server group, or AZ. You can view only the Layer 7 metrics of a backend server group.

Table 1-73 Metrics supported by each dedicated load balancer

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m1_cps	Concurrent Connections	Load balancing at Layer 4: total number of TCP and UDP connections from the monitored object to backend servers. Load balancing at Layer 7: total number of TCP connections from the clients to the monitored object. Unit: Count	≥ 0	Dedicated load balancer	1 minute
m2_act_conn	Active Connections	Number of TCP and UDP connections in the ESTABLISHED state between the monitored object and backend servers. You can run the following command to view the connections (both Windows and Linux servers): <code>netstat -an</code> Unit: Count	≥ 0	Dedicated load balancer	1 minute
m3_inact_conn	Inactive Connections	Number of TCP connections between the monitored object and backend servers except those in the ESTABLISHED state. You can run the following command to view the connections (both Windows and Linux servers): <code>netstat -an</code> Unit: Count	≥ 0	Dedicated load balancer	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m4_ncps	New Connections	Number of connections established between clients and the monitored object per second. Unit: packets/s	$\geq 0/s$	Dedicated load balancer	1 minute
m5_inpps	Incoming Packets	Number of packets received by the monitored object per second. Unit: packets/s	$\geq 0/s$	Dedicated load balancer	1 minute
m6_outpps	Outgoing Packets	Number of packets sent from the monitored object per second. Unit: packets/s	$\geq 0/s$	Dedicated load balancer	1 minute
m7_in_Bps	Inbound Rate	Traffic used for accessing the monitored object from the Internet. Unit: bytes/s	≥ 0 byte/s	Dedicated load balancer	1 minute
m8_out_Bps	Outbound Rate	Traffic used by the monitored object to access the Internet per second. Unit: bytes/s	≥ 0 byte/s	Dedicated load balancer	1 minute
m9_abnormal_servers	Unhealthy Servers	Number of unhealthy backend servers associated with the monitored object. Unit: Count	≥ 0	Dedicated load balancer	1 minute
ma_normal_servers	Healthy Servers	Number of healthy backend servers associated with the monitored object. Unit: Count	≥ 0	Dedicated load balancer	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m22_in_bandwidth	Inbound Bandwidth	Bandwidth used for accessing the monitored object from the Internet. Unit: bits/s	≥ 0 bit/s	Dedicated load balancer	1 minute
m23_out_bandwidth	Outbound Bandwidth	Bandwidth used by the monitored object to access the Internet. Unit: bits/s	≥ 0 bit/s	Dedicated load balancer	1 minute
m26_in_bandwidth_ipv6	IPv6 Inbound Bandwidth	IPv6 network bandwidth used for accessing the monitored object from the Internet. Unit: bits/s	≥ 0 bit/s	Dedicated load balancer	1 minute
m27_out_bandwidth_ipv6	IPv6 Outbound Bandwidth	IPv6 network bandwidth used by the monitored object to access the Internet. Unit: bits/s	≥ 0 bit/s	Dedicated load balancer	1 minute
m1e_server_rps	Reset Packets from Backend Servers	Number of reset packets sent from backend servers to clients. These reset packets are generated by the backend servers and then forwarded by the load balancer. Supported protocols: TCP Unit: Count/s	≥ 0 /s	Dedicated load balancer	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m21_client_rps	Reset Packets from Clients	Number of reset packets sent by clients to backend servers. These reset packets are generated by clients and then forwarded by the load balancer. Supported protocols: TCP Unit: Count/s	$\geq 0/s$	Dedicated load balancer	1 minute
m1f_lvs_rps	Reset Packets from Load Balancers	Number of reset packets generated by the load balancer. Supported protocols: TCP Unit: Count/s	$\geq 0/s$	Dedicated load balancer	1 minute
mb_l7_queries	Layer-7 Query Rate	Number of requests the monitored object receives per second. Supported protocol: HTTP/HTTPS/QUIC Unit: Count/s	$\geq 0/s$	Dedicated load balancer	1 minute
mc_l7_http_2xx	Layer-7 2xx Status Codes	Number of 2xx status codes returned by the load balancer and backend servers. Supported protocol: HTTP/HTTPS/QUIC Unit: Count/s	$\geq 0/s$	Dedicated load balancer	1 minute
md_l7_http_3xx	Layer-7 3xx Status Codes	Number of 3xx status codes returned by the load balancer and backend servers. Supported protocol: HTTP/HTTPS/QUIC Unit: Count/s	$\geq 0/s$	Dedicated load balancer	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
me_l7_http_4xx	Layer-7 4xx Status Codes	Number of 4xx status codes returned by the load balancer and backend servers. Supported protocol: HTTP/HTTPS/QUIC Unit: Count/s	$\geq 0/s$	Dedicated load balancer	1 minute
mf_l7_http_5xx	Layer-7 5xx Status Codes	Number of 5xx status codes returned by the load balancer and backend servers. Supported protocol: HTTP/HTTPS/QUIC Unit: Count/s	$\geq 0/s$	Dedicated load balancer	1 minute
m10_l7_http_other_status	Layer-7 Other Status Codes	Number of status codes returned by the load balancer and backend servers except 2xx, 3xx, 4xx, and 5xx status codes. Supported protocol: HTTP/HTTPS/QUIC Unit: Count/s	$\geq 0/s$	Dedicated load balancer	1 minute
m11_l7_http_404	Layer-7 404 Not Found	Number of 404 Not Found status codes returned by the load balancer and backend servers. Supported protocol: HTTP/HTTPS/QUIC Unit: Count/s	$\geq 0/s$	Dedicated load balancer	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m12_l7_http_499	Layer-7 499 Client Closed Request	Number of 499 Client Closed Request status codes returned by the load balancer and backend servers. Supported protocol: HTTP/HTTPS/QUIC Unit: Count/s	$\geq 0/s$	Dedicated load balancer	1 minute
m13_l7_http_502	Layer-7 502 Bad Gateway	Number of 502 Bad Gateway status codes returned by the load balancer and backend servers. Supported protocol: HTTP/HTTPS/QUIC Unit: Count/s	$\geq 0/s$	Dedicated load balancer	1 minute
m14_l7_rt	Average Layer-7 Response Time	Average response time of the monitored object. Supported protocol: HTTP/HTTPS/QUIC The response time starts when the monitored object receives requests from the clients and ends when it returns all responses to the clients. Unit: ms NOTE The average response time it takes to establish a WebSocket connection may be very long. This metric cannot be used as a reference.	≥ 0 ms	Dedicated load balancer	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m15_l7_upstream_4xx	4xx Status Codes Backend	Number of 4xx status codes returned by the backend servers. Supported protocol: HTTP/HTTPS/QUIC Unit: Count/s	$\geq 0/s$	Dedicated load balancer	1 minute
m16_l7_upstream_5xx	5xx Status Codes Backend	Number of 5xx status codes returned by the backend servers. Supported protocol: HTTP/HTTPS/QUIC Unit: Count/s	$\geq 0/s$	Dedicated load balancer	1 minute
m17_l7_upstream_rt	Average Server Response Time	Average response time of backend servers. The response time starts when the monitored object routes the requests to the backend server and ends when the monitored object receives a response from the backend server. Supported protocol: HTTP/HTTPS/QUIC Unit: ms NOTE The average response time it takes to establish a WebSocket connection may be very long. This metric cannot be used as a reference.	≥ 0 ms	Dedicated load balancer	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m1a_l7_upstream_rt_max	Maximum Server Response Time	<p>Maximum response time of backend servers.</p> <p>The response time starts when the monitored object routes the requests to the backend server and ends when the monitored object receives a response from the backend server.</p> <p>Supported protocol: HTTP/HTTPS/QUIC</p> <p>Unit: ms</p>	≥ 0 ms	Dedicated load balancer	1 minute
m1b_l7_upstream_rt_min	Minimum Server Response Time	<p>Minimum response time of backend servers.</p> <p>The response time starts when the monitored object routes the requests to the backend server and ends when the monitored object receives a response from the backend server.</p> <p>Supported protocol: HTTP/HTTPS/QUIC</p> <p>Unit: ms</p>	≥ 0 ms	Dedicated load balancer	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m1c_l7_rt_max	Maximum Layer-7 Response Time	<p>Maximum response time of the monitored object.</p> <p>The response time starts when the monitored object receives requests from the clients and ends when it returns all responses to the clients.</p> <p>Supported protocol: HTTP/HTTPS/QUIC</p> <p>Unit: ms</p>	≥ 0 ms	Dedicated load balancer	1 minute
m1d_l7_rt_min	Minimum Layer-7 Response Time	<p>Minimum response time of the monitored object.</p> <p>The response time starts when the monitored object receives requests from the clients and ends when it returns all responses to the clients.</p> <p>Supported protocol: HTTP/HTTPS/QUIC</p> <p>Unit: ms</p>	≥ 0 ms	Dedicated load balancer	1 minute
m25_l7_resp_Bps	Backend Server Response Bandwidth	<p>The bandwidth that the monitored object uses to return response to clients.</p> <p>Supported protocol: HTTP/HTTPS/QUIC</p> <p>Unit: bits/s</p> <p>NOTE</p> <p>When HTTP/2 is enabled for a listener, this metric cannot be used as a reference.</p>	≥ 0 bit/s	Dedicated load balancer	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m24_l7_req_Bps	Backend Server Request Bandwidth	<p>The bandwidth that the monitored object uses to receive requests from clients.</p> <p>Supported protocol: HTTP/HTTPS/QUIC</p> <p>Unit: bits/s</p> <p>NOTE When HTTP/2 is enabled for a listener, this metric cannot be used as a reference.</p>	≥ 0 bit/s	Dedicated load balancer	1 minute
l7_con_usage	Layer-7 Concurrent Connection Usage	<p>Ratio of HTTP and HTTPS connections established between the monitored object and backend servers per second, to the maximum number of concurrent connections allowed per second.</p> <p>Unit: percentage (%)</p>	≥ 0%	Dedicated load balancer	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
l7_in_bps_usage	Layer-7 Inbound Bandwidth Usage	<p>Ratio of the bandwidth that the monitored object uses to receive requests from clients over HTTP and HTTPS, to the maximum inbound bandwidth allowed.</p> <p>Unit: percentage (%)</p> <p>CAUTION If the inbound bandwidth usage reaches 100%, the load balancer performance has reached the upper limit. If the inbound bandwidth keeps higher than the bandwidth that the load balancer can provide, the service availability cannot be guaranteed.</p>	≥ 0%	Dedicated load balancer	1 minute
l7_out_bps_usage	Layer-7 Outbound Bandwidth Usage	<p>Ratio of the bandwidth that the monitored object uses to return response to clients over HTTP and HTTPS, to the maximum outbound bandwidth allowed.</p> <p>Unit: percentage (%)</p> <p>CAUTION If the outbound bandwidth usage reaches 100%, the load balancer performance has reached the upper limit. If the outbound bandwidth keeps higher than the bandwidth that the load balancer can provide, the service availability cannot be guaranteed.</p>	≥ 0%	Dedicated load balancer	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
l7_ncps_usage	Layer-7 New Connection Usage	Ratio of HTTP and HTTPS connections established between clients and the monitored object per second, to the maximum number of new connections allowed per second. Unit: percentage (%)	$\geq 0\%$	Dedicated load balancer	1 minute
l7_qps_usage	Layer 7 QPS Usage	Ratio of HTTP and HTTPS queries per second on the monitored object, to the maximum number of queries allowed per second. Unit: percentage (%)	$\geq 0\%$	Dedicated load balancer	1 minute
l4_con_usage	Layer-4 Concurrent Connection Usage	Ratio of TCP and UDP connections established between the monitored object and backend servers per second, to the maximum number of concurrent connections allowed per second. Unit: percentage (%)	$\geq 0\%$	Dedicated load balancer	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
l4_in_bps_usage	Layer-4 Inbound Bandwidth Usage	<p>Ratio of the bandwidth that the monitored object uses to receive requests from clients over TCP and UDP, to the maximum inbound bandwidth allowed.</p> <p>Unit: percentage (%)</p> <p>CAUTION If the inbound bandwidth usage reaches 100%, the load balancer performance has reached the upper limit. If the inbound bandwidth keeps higher than the bandwidth that the load balancer can provide, the service availability cannot be guaranteed.</p>	≥ 0%	Dedicated load balancer	1 minute
l4_out_bps_usage	Layer-4 Outbound Bandwidth Usage	<p>Ratio of the bandwidth that the monitored object uses to return response to clients over TCP and UDP, to the maximum outbound bandwidth allowed.</p> <p>Unit: percentage (%)</p> <p>CAUTION If the outbound bandwidth usage reaches 100%, the load balancer performance has reached the upper limit. If the outbound bandwidth keeps higher than the bandwidth that the load balancer can provide, the service availability cannot be guaranteed.</p>	≥ 0%	Dedicated load balancer	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
l4_ncps_usage	Layer-4 New Connection Usage	Ratio of TCP and UDP connections established between clients and the monitored object per second, to the maximum number of new connections allowed per second. Unit: percentage (%)	$\geq 0\%$	Dedicated load balancer	1 minute
ipgroup_blocked_packets	Blocked Packets	Number of incoming packets blocked from the monitored object per second. Unit: Count/s	$\geq 0/s$	Dedicated load balancer	1 minute
ipgroup_blocked_traffic	Blocked Traffic	Incoming traffic blocked from the monitored object per second. Unit: bits/s	$\geq 0 \text{ bit/s}$	Dedicated load balancer	1 minute
dropped_connections	Dropped Connections	Number of connections dropped by the monitored object per second. Unit: Count/s	$\geq 0/s$	Dedicated load balancer	1 minute
dropped_packets	Dropped Packets	Number of packets dropped by the monitored object per second. Unit: Count/s	$\geq 0/s$	Dedicated load balancer	1 minute
dropped_traffic	Discarded Traffic	Traffic discarded by the monitored object per second. Unit: bits/s	$\geq 0 \text{ bit/s}$	Dedicated load balancer	1 minute

Listener Metrics

Table 1-74 Metrics supported by each listener

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m1_cps	Concurrent Connections	<p>Load balancing at Layer 4: total number of TCP and UDP connections from the monitored object to backend servers.</p> <p>Load balancing at Layer 7: total number of TCP connections from the clients to the monitored object.</p> <p>Unit: Count</p>	≥ 0	Dedicated load balancer - listener	1 minute
m2_act_conn	Active Connections	<p>Number of TCP and UDP connections in the ESTABLISHED state between the monitored object and backend servers.</p> <p>You can run the following command to view the connections (both Windows and Linux servers): netstat -an</p> <p>Unit: Count</p>	≥ 0	Dedicated load balancer - listener	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m3_inact_conn	Inactive Connections	Number of TCP connections between the monitored object and backend servers except those in the ESTABLISHED state. You can run the following command to view the connections (both Windows and Linux servers): netstat -an Unit: Count	≥ 0	Dedicated load balancer - listener	1 minute
m4_ncps	New Connections	Number of connections established between clients and the monitored object per second. Unit: Count/s	$\geq 0/s$	Dedicated load balancer - listener	1 minute
m5_in_pps	Incoming Packets	Number of packets received by the monitored object per second. Unit: Count/s	$\geq 0/s$	Dedicated load balancer - listener	1 minute
m6_out_pps	Outgoing Packets	Number of packets sent from the monitored object per second. Unit: Count/s	$\geq 0/s$	Dedicated load balancer - listener	1 minute
m7_in_Bps	Inbound Rate	Traffic used for accessing the monitored object from the Internet. Unit: bytes/s	≥ 0 byte/s	Dedicated load balancer - listener	1 minute
m8_out_Bps	Outbound Rate	Traffic used by the monitored object to access the Internet per second. Unit: bytes/s	≥ 0 byte/s	Dedicated load balancer - listener	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m9_abnormal_servers	Unhealthy Servers	Number of unhealthy backend servers associated with the monitored object. Unit: Count	≥ 0	Dedicated load balancer - listener	1 minute
ma_normal_servers	Healthy Servers	Number of healthy backend servers associated with the monitored object. Unit: Count	≥ 0	Dedicated load balancer - listener	1 minute
m22_in_bandwidth	Inbound Bandwidth	Bandwidth used for accessing the monitored object from the Internet. Unit: bits/s	≥ 0 bit/s	Dedicated load balancer - listener	1 minute
m23_out_bandwidth	Outbound Bandwidth	Bandwidth used by the monitored object to access the Internet. Unit: bits/s	≥ 0 bit/s	Dedicated load balancer - listener	1 minute
m1e_server_rps	Reset Packets from Backend Servers	Number of reset packets sent from backend servers to clients. These reset packets are generated by the backend servers and then forwarded by the load balancer. Supported protocols: TCP Unit: Count/s	$\geq 0/s$	Dedicated load balancer - listener	1 minute
m21_client_rps	Reset Packets from Clients	Number of reset packets sent by clients to backend servers. These reset packets are generated by clients and then forwarded by the load balancer. Supported protocols: TCP Unit: Count/s	$\geq 0/s$	Dedicated load balancer - listener	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m1f_lvs_rps	Reset Packets from Load Balancers	Number of reset packets generated by the load balancer. Supported protocols: TCP Unit: Count/s	$\geq 0/s$	Dedicated load balancer - listener	1 minute
mb_l7_qps	Layer-7 Query Rate	Number of requests the monitored object receives per second. Supported protocols: HTTP/HTTPS Unit: Count/s	$\geq 0/s$	Dedicated load balancer - listener	1 minute
mc_l7_http_2xx	Layer-7 2xx Status Codes	Number of 2xx status codes returned by the load balancer and backend servers. Supported protocols: HTTP/HTTPS Unit: Count/s	$\geq 0/s$	Dedicated load balancer - listener	1 minute
md_l7_http_3xx	Layer-7 3xx Status Codes	Number of 3xx status codes returned by the load balancer and backend servers. Supported protocols: HTTP/HTTPS Unit: Count/s	$\geq 0/s$	Dedicated load balancer - listener	1 minute
me_l7_http_4xx	Layer-7 4xx Status Codes	Number of 4xx status codes returned by the load balancer and backend servers. Supported protocols: HTTP/HTTPS Unit: Count/s	$\geq 0/s$	Dedicated load balancer - listener	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
mf_l7_http_5xx	Layer-7 5xx Status Codes	Number of 5xx status codes returned by the load balancer and backend servers. Supported protocols: HTTP/HTTPS Unit: Count/s	$\geq 0/s$	Dedicated load balancer - listener	1 minute
m10_l7_http_other_status	Layer-7 Other Status Codes	Number of status codes returned by the load balancer and backend servers except 2xx, 3xx, 4xx, and 5xx status codes. Supported protocols: HTTP/HTTPS Unit: Count/s	$\geq 0/s$	Dedicated load balancer - listener	1 minute
m11_l7_http_404	Layer-7 404 Not Found	Number of 404 Not Found status codes returned by the load balancer and backend servers. Supported protocols: HTTP/HTTPS Unit: Count/s	$\geq 0/s$	Dedicated load balancer - listener	1 minute
m12_l7_http_499	Layer-7 499 Client Closed Request	Number of 499 Client Closed Request status codes returned by the load balancer and backend servers. Supported protocols: HTTP/HTTPS Unit: Count/s	$\geq 0/s$	Dedicated load balancer - listener	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m13_l7_http_502	Layer-7 502 Bad Gateway	Number of 502 Bad Gateway status codes returned by the load balancer and backend servers. Supported protocols: HTTP/HTTPS Unit: Count/s	$\geq 0/s$	Dedicated load balancer - listener	1 minute
m14_l7_rt	Average Layer-7 Response Time	Average response time of the monitored object. Supported protocols: HTTP/HTTPS The response time starts when the monitored object receives requests from the clients and ends when it returns all responses to the clients. Unit: ms NOTE The average response time it takes to establish a WebSocket connection may be very long. This metric cannot be used as a reference.	≥ 0 ms	Dedicated load balancer - listener	1 minute
m15_l7_upstream_4xx	4xx Status Codes Backend	Number of 4xx status codes returned by the backend servers. Supported protocols: HTTP/HTTPS Unit: Count/s	$\geq 0/s$	Dedicated load balancer - listener	1 minute
m16_l7_upstream_5xx	5xx Status Codes Backend	Number of 5xx status codes returned by the monitored object. Supported protocols: HTTP/HTTPS Unit: Count/s	$\geq 0/s$	Dedicated load balancer - listener	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m17_l7_upstream_rt	Average Server Response Time	<p>Average response time of backend servers.</p> <p>Supported protocols: HTTP/HTTPS</p> <p>The response time starts when the monitored object routes the requests to the backend server and ends when the monitored object receives a response from the backend server.</p> <p>Unit: ms</p> <p>NOTE The average response time it takes to establish a WebSocket connection may be very long. This metric cannot be used as a reference.</p>	≥ 0 ms	Dedicated load balancer - listener	1 minute
m1a_l7_upstream_rt_max	Maximum Server Response Time	<p>Maximum response time of backend servers.</p> <p>Supported protocols: HTTP/HTTPS</p> <p>The response time starts when the monitored object routes the requests to the backend server and ends when the monitored object receives a response from the backend server.</p> <p>Unit: ms</p>	≥ 0 ms	Dedicated load balancer - listener	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m1b_l7_upstream_rt_min	Minimum Server Response Time	Minimum response time of backend servers. Supported protocols: HTTP/HTTPS The response time starts when the monitored object routes the requests to the backend server and ends when the monitored object receives a response from the backend server. Unit: ms	≥ 0 ms	Dedicated load balancer - listener	1 minute
m1c_l7_rt_max	Maximum Layer-7 Response Time	Maximum response time of the monitored object. Supported protocols: HTTP/HTTPS The response time starts when the monitored object receives requests from the clients and ends when it returns all responses to the clients. Unit: ms	≥ 0 ms	Dedicated load balancer - listener	1 minute
m1d_l7_rt_min	Minimum Layer-7 Response Time	Minimum response time of the monitored object. Supported protocols: HTTP/HTTPS The response time starts when the monitored object receives requests from the clients and ends when it returns all responses to the clients. Unit: ms	≥ 0 ms	Dedicated load balancer - listener	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
ipgroup_blocked_packets	Blocked Packets	Number of incoming packets blocked from the monitored object per second. Unit: Count/s	$\geq 0/s$	Dedicated load balancer - listener	1 minute
ipgroup_blocked_traffic	Blocked Traffic	Incoming traffic blocked from the monitored object per second. Unit: bits/s	≥ 0 bit/s	Dedicated load balancer - listener	1 minute

Backend Server Group Metrics

Table 1-75 Metrics supported by each backend server group

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m9_abnormal_servers	Unhealthy Servers	Number of unhealthy backend servers associated with the monitored object. Unit: Count	≥ 0	Dedicated load balancer - backend server group	1 minute
ma_normal_servers	Healthy Servers	Number of healthy backend servers associated with the monitored object. Unit: Count	≥ 0	Dedicated load balancer - backend server group	1 minute
mb_l7_queries	Layer-7 Query Rate	Number of requests the monitored object receives per second. Unit: Count/s	$\geq 0/s$	Dedicated load balancer - backend server group	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m17_l7_upstream_rt	Average Server Response Time	<p>Average response time of backend servers.</p> <p>Supported protocols: HTTP/HTTPS</p> <p>The response time starts when the monitored object routes the requests to the backend server and ends when the monitored object receives a response from the backend server.</p> <p>Unit: ms</p> <p>NOTE The average response time it takes to establish a WebSocket connection may be very long. This metric cannot be used as a reference.</p>	≥ 0 ms	Dedicated load balancer - backend server group	1 minute
m1a_l7_upstream_rt_max	Maximum Server Response Time	<p>Maximum response time of backend servers.</p> <p>Supported protocols: HTTP/HTTPS</p> <p>The response time starts when the monitored object routes the requests to the backend server and ends when the monitored object receives a response from the backend server.</p> <p>Unit: ms</p>	≥ 0 ms	Dedicated load balancer - backend server group	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m1b_l7_upstream_rt_min	Minimum Server Response Time	<p>Minimum response time of backend servers.</p> <p>Supported protocols: HTTP/HTTPS</p> <p>The response time starts when the monitored object routes the requests to the backend server and ends when the monitored object receives a response from the backend server.</p> <p>Unit: ms</p>	≥ 0 ms	Dedicated load balancer - backend server group	1 minute
m18_l7_upstream_2xx	2xx Status Codes Backend	<p>Number of 2xx status codes returned by the backend servers.</p> <p>Supported protocols: HTTP/HTTPS</p> <p>Unit: Count/s</p>	≥ 0 /s	Dedicated load balancer - backend server group	1 minute
m19_l7_upstream_3xx	3xx Status Codes Backend	<p>Number of 3xx status codes returned by the backend servers.</p> <p>Supported protocols: HTTP/HTTPS</p> <p>Unit: Count/s</p>	≥ 0 /s	Dedicated load balancer - backend server group	1 minute
m15_l7_upstream_4xx	4xx Status Codes Backend	<p>Number of 4xx status codes returned by the backend servers.</p> <p>Supported protocols: HTTP/HTTPS</p> <p>Unit: Count/s</p>	≥ 0 /s	Dedicated load balancer - backend server group	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m16_l7_upstream_5xx	5xx Status Codes Backend	Number of 5xx status codes returned by the monitored object. Supported protocols: HTTP/HTTPS Unit: Count/s	$\geq 0/s$	Dedicated load balancer - backend server group	1 minute
m25_l7_resp_Bps	Backend Server Response Bandwidth	The bandwidth that the monitored object uses to return response to clients. Unit: bits/s NOTE When HTTP/2 is enabled for a listener, this metric cannot be used as a reference.	$\geq 0 \text{ bit/s}$	Dedicated load balancer - backend server group	1 minute
m24_l7_req_Bps	Backend Server Request Bandwidth	The bandwidth that the monitored object uses to receive requests from clients. Unit: bits/s NOTE When HTTP/2 is enabled for a listener, this metric cannot be used as a reference.	$\geq 0 \text{ bit/s}$	Dedicated load balancer - backend server group	1 minute

AZ Metrics

Table 1-76 AZ metrics

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m1_cps	Concurrent Connections	Load balancing at Layer 4: total number of TCP and UDP connections from the monitored object to backend servers. Load balancing at Layer 7: total number of TCP connections from the clients to the monitored object. Unit: Count	≥ 0	AZ	1 minute
m2_act_conn	Active Connections	Number of TCP and UDP connections in the ESTABLISHED state between the monitored object and backend servers. You can run the following command to view the connections (both Windows and Linux servers): <code>netstat -an</code> Unit: Count	≥ 0	AZ	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m3_inact_conn	Inactive Connections	Number of TCP connections between the monitored object and backend servers except those in the ESTABLISHED state. You can run the following command to view the connections (both Windows and Linux servers): <code>netstat -an</code> Unit: Count	≥ 0	AZ	1 minute
m4_ncps	New Connections	Number of connections established between clients and the monitored object per second. Unit: packets/s	$\geq 0/s$	AZ	1 minute
m5_inpps	Incoming Packets	Number of packets received by the monitored object per second. Unit: Count/s	$\geq 0/s$	AZ	1 minute
m6_outpps	Outgoing Packets	Number of packets sent from the monitored object per second. Unit: Count/s	$\geq 0/s$	AZ	1 minute
m7_in_Bps	Inbound Rate	Traffic used for accessing the monitored object from the Internet. Unit: bytes/s	≥ 0 byte/s	AZ	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m8_out_Bps	Outbound Rate	Traffic used by the monitored object to access the Internet per second. Unit: bytes/s	≥ 0 byte/s	AZ	1 minute
m26_in_bandwidth_ipv6	IPv6 Inbound Bandwidth	IPv6 network bandwidth used for accessing the monitored object from the Internet. Unit: bits/s	≥ 0 bit/s	AZ	1 minute
m27_out_bandwidth_ipv6	IPv6 Outbound Bandwidth	IPv6 network bandwidth used by the monitored object to access the Internet. Unit: bits/s	≥ 0 bit/s	AZ	1 minute
m1e_server_rps	Reset Packets from Backend Servers	Number of reset packets sent from backend servers to clients. These reset packets are generated by the backend servers and then forwarded by the load balancer. Supported protocols: TCP Unit: Count/s	$\geq 0/s$	AZ	1 minute
m21_client_rps	Reset Packets from Clients	Number of reset packets sent by clients to backend servers. These reset packets are generated by clients and then forwarded by the load balancer. Supported protocols: TCP Unit: Count/s	$\geq 0/s$	AZ	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m1f_lvs_rps	Reset Packets from Load Balancers	Number of reset packets generated by the load balancer. Supported protocols: TCP Unit: Count/s	$\geq 0/s$	AZ	1 minute
mb_l7_qps	Layer-7 Query Rate	Number of requests the monitored object receives per second. Supported protocols: HTTP/HTTPS Unit: Count/s	$\geq 0/s$	AZ	1 minute
mc_l7_http_2xx	Layer-7 2xx Status Codes	Number of 2xx status codes returned by the load balancer and backend servers. Supported protocols: HTTP/HTTPS Unit: Count/s	$\geq 0/s$	AZ	1 minute
md_l7_http_3xx	Layer-7 3xx Status Codes	Number of 3xx status codes returned by the load balancer and backend servers. Supported protocols: HTTP/HTTPS Unit: Count/s	$\geq 0/s$	AZ	1 minute
me_l7_http_4xx	Layer-7 4xx Status Codes	Number of 4xx status codes returned by the load balancer and backend servers. Supported protocols: HTTP/HTTPS Unit: Count/s	$\geq 0/s$	AZ	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
mf_l7_http_5xx	Layer-7 5xx Status Codes	Number of 5xx status codes returned by the load balancer and backend servers. Supported protocols: HTTP/HTTPS Unit: Count/s	$\geq 0/s$	AZ	1 minute
m10_l7_http_other_statuses	Layer-7 Other Status Codes	Number of status codes returned by the load balancer and backend servers except 2xx, 3xx, 4xx, and 5xx status codes. Supported protocols: HTTP/HTTPS Unit: Count/s	$\geq 0/s$	AZ	1 minute
m11_l7_http_404	Layer-7 404 Not Found	Number of 404 Not Found status codes returned by the load balancer and backend servers. Supported protocols: HTTP/HTTPS Unit: Count/s	$\geq 0/s$	AZ	1 minute
m12_l7_http_499	Layer-7 499 Client Closed Request	Number of 499 Client Closed Request status codes returned by the load balancer and backend servers. Supported protocols: HTTP/HTTPS Unit: Count/s	$\geq 0/s$	AZ	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m13_l7_http_502	Layer-7 502 Bad Gateway	Number of 502 Bad Gateway status codes returned by the load balancer and backend servers. Supported protocols: HTTP/HTTPS Unit: Count/s	$\geq 0/s$	AZ	1 minute
m14_l7_rt	Average Layer-7 Response Time	Average response time of the monitored object. Supported protocols: HTTP/HTTPS The response time starts when the monitored object receives requests from the clients and ends when it returns all responses to the clients. Unit: ms NOTE The average response time it takes to establish a WebSocket connection may be very long. This metric cannot be used as a reference.	≥ 0 ms	AZ	1 minute
m15_l7_upstream_4xx	4xx Status Codes Backend	Number of 4xx status codes returned by the backend servers. Supported protocols: HTTP/HTTPS Unit: Count/s	$\geq 0/s$	AZ	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m16_l7_upstream_5xx	5xx Status Codes Backend	Number of 5xx status codes returned by the backend servers. Supported protocols: HTTP/HTTPS Unit: Count/s	≥ 0/s	AZ	1 minute
m17_l7_upstream_rt	Average Server Response Time	Average response time of backend servers. The response time starts when the monitored object routes the requests to the backend server and ends when the monitored object receives a response from the backend server. Supported protocols: HTTP/HTTPS Unit: ms NOTE The average response time it takes to establish a WebSocket connection may be very long. This metric cannot be used as a reference.	≥ 0 ms	AZ	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m1a_l7_upstream_rt_max	Maximum Server Response Time	<p>Maximum response time of backend servers.</p> <p>The response time starts when the monitored object routes the requests to the backend server and ends when the monitored object receives a response from the backend server.</p> <p>Supported protocols: HTTP/HTTPS</p> <p>Unit: ms</p>	≥ 0 ms	AZ	1 minute
m1b_l7_upstream_rt_min	Minimum Server Response Time	<p>Minimum response time of backend servers.</p> <p>The response time starts when the monitored object routes the requests to the backend server and ends when the monitored object receives a response from the backend server.</p> <p>Supported protocols: HTTP/HTTPS</p> <p>Unit: ms</p>	≥ 0 ms	AZ	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m1c_l7_rt_max	Maximum Layer-7 Response Time	<p>Maximum response time of the monitored object.</p> <p>The response time starts when the monitored object receives requests from the clients and ends when it returns all responses to the clients.</p> <p>Supported protocols: HTTP/HTTPS</p> <p>Unit: ms</p>	≥ 0 ms	AZ	1 minute
m1d_l7_rt_min	Minimum Layer-7 Response Time	<p>Minimum response time of the monitored object.</p> <p>The response time starts when the monitored object receives requests from the clients and ends when it returns all responses to the clients.</p> <p>Supported protocols: HTTP/HTTPS</p> <p>Unit: ms</p>	≥ 0 ms	AZ	1 minute
l4_con_usage	Layer-4 Concurrent Connection Usage	<p>Ratio of TCP and UDP connections established between the monitored object and backend servers per second, to the maximum number of concurrent connections allowed per second.</p> <p>Unit: percentage (%)</p>	$\geq 0\%$	AZ	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
l4_in_bps_usage	Layer-4 Inbound Bandwidth Usage	<p>Ratio of the bandwidth that the monitored object uses to receive requests from clients over TCP and UDP, to the maximum inbound bandwidth allowed.</p> <p>Unit: percentage (%)</p> <p>CAUTION If the inbound bandwidth usage reaches 100%, the load balancer performance has reached the upper limit. If the inbound bandwidth keeps higher than the bandwidth that the load balancer can provide, the service availability cannot be guaranteed.</p>	≥ 0%	AZ	1 minute
l4_out_bps_usage	Layer-4 Outbound Bandwidth Usage	<p>Ratio of the bandwidth that the monitored object uses to return response to clients over TCP and UDP, to the maximum outbound bandwidth allowed.</p> <p>Unit: percentage (%)</p> <p>CAUTION If the outbound bandwidth usage reaches 100%, the load balancer performance has reached the upper limit. If the outbound bandwidth keeps higher than the bandwidth that the load balancer can provide, the service availability cannot be guaranteed.</p>	≥ 0%	AZ	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
l4_ncps_usage	Layer-4 New Connection Usage	Ratio of TCP and UDP connections established between clients and the monitored object per second, to the maximum number of new connections allowed per second. Unit: percentage (%)	≥ 0%	AZ	1 minute
l7_in_bps_usage	Layer-7 Inbound Bandwidth Usage	Ratio of the bandwidth that the monitored object uses to receive requests from clients over HTTP and HTTPS, to the maximum inbound bandwidth allowed. Unit: percentage (%) CAUTION If the inbound bandwidth usage reaches 100%, the load balancer performance has reached the upper limit. If the inbound bandwidth keeps higher than the bandwidth that the load balancer can provide, the service availability cannot be guaranteed.	≥ 0%	AZ	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
l7_out_bps_usage	Layer-7 Outbound Bandwidth Usage	Ratio of the bandwidth that the monitored object uses to return response to clients over HTTP and HTTPS, to the maximum outbound bandwidth allowed. Unit: percentage (%) CAUTION If the outbound bandwidth usage reaches 100%, the load balancer performance has reached the upper limit. If the outbound bandwidth keeps higher than the bandwidth that the load balancer can provide, the service availability cannot be guaranteed.	$\geq 0\%$	AZ	1 minute
l7_con_usage	Layer-7 Concurrent Connection Usage	Ratio of HTTP and HTTPS connections established between the monitored object and backend servers per second, to the maximum number of concurrent connections allowed per second. Unit: percentage (%)	$\geq 0\%$	AZ	1 minute
l7_ncps_usage	Layer-7 New Connection Usage	Ratio of HTTP and HTTPS connections established between clients and the monitored object per second, to the maximum number of new connections allowed per second. Unit: percentage (%)	$\geq 0\%$	AZ	1 minute

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
l7_qps_usage	Layer 7 QPS Usage	Ratio of HTTP and HTTPS queries per second on the monitored object, to the maximum number of queries allowed per second. Unit: percentage (%)	≥ 0%	AZ	1 minute

Dimensions

Key	Value
lbaas_instance_id	ID of a dedicated load balancer.
lbaas_listener_id	ID of a listener added to a dedicated load balancer.
lbaas_pool_id	ID of a backend server group.
available_zone	AZ where a dedicated load balancer works.

1.11.3 Event Monitoring

Overview

You can query system events that are automatically reported to Cloud Eye and custom events reported to Cloud Eye through the API. When there are specified events, you will receive alarm notifications.

Events are key operations on ELB resources that are stored and monitored by Cloud Eye. You can view events to see operations performed by specific users on specific ELB resources.

Event monitoring provides an API for reporting custom events, which helps you collect and report abnormal events or important change events generated by ELB to Cloud Eye.

Event monitoring is enabled by default and allows you to view monitoring details of system events and custom events. For operations supported by event monitoring, see [Monitoring Events Supported by ELB](#).

Monitoring Events Supported by ELB

[Table 1-77](#) lists the monitoring events supported by dedicated load balancers.

Table 1-77 Monitoring events supported by dedicated load balancers

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
ELB	The backend servers are unhealthy.	healthCheckUnhealthy	Major	Generally, this problem occurs because the backend servers are offline. This event will not be reported after it is reported for several times.	Check whether the backend servers are running properly.	ELB does not forward requests to unhealthy backend servers. If all backend servers in the backend server group are detected unhealthy, services will be interrupted.
	The backend server is detected healthy.	healthCheckRecovery	Minor	The backend server is detected healthy.	No further action is required.	The load balancer routes requests to this backend server.

1.11.4 Viewing Traffic Usage

Scenarios

For livestreaming platforms, traffic often increases suddenly, which makes the services unstable. To address this issue, most of them use ELB to distribute traffic. By working with Cloud Eye, ELB allows you to monitor the traffic usage in real time. You can view the traffic consumed by the EIPs bound to public network load balancers to better balance your application workloads.

Prerequisites

Load balancers are running properly.

The associated backend servers are running normally and are not deleted or in the stopped or faulty state.

Viewing Traffic Usage of the Bound EIP



1. Log in to the management console.
2. In the upper left corner of the page, click  and select the desired region and project.
3. Click  in the upper left corner of the page and choose **Networking > Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Elastic IP and Bandwidth > EIPs**.
5. Locate the EIP bound to the load balancer and click its name. On the **Bandwidth** tab, you can view the data for the last 1, 3, 12 hours, last day, or last 7 days.

Figure 1-40 EIP traffic usage

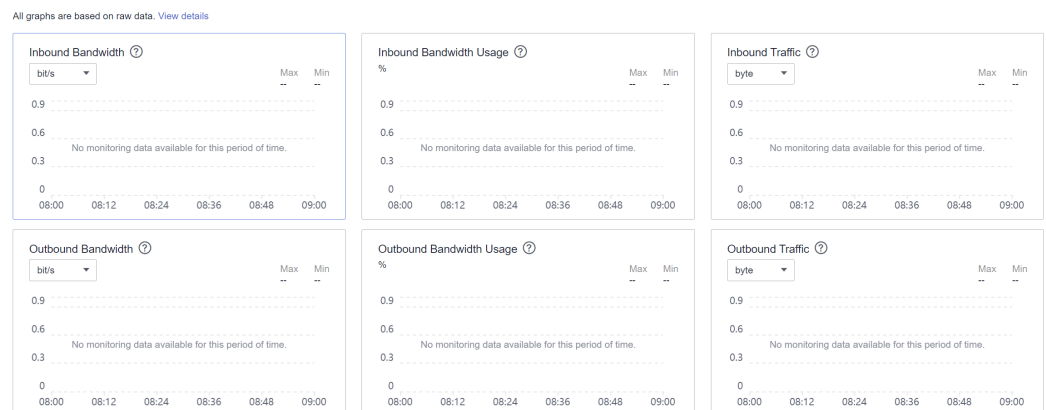


Table 1-78 EIP and bandwidth metrics

Metric	Meaning	Value Range	Monitored Object	Monitoring Period (Raw Data)
Outbound Bandwidth (originally named "Upstream Bandwidth")	Network rate of outbound traffic	≥ 0 bits/s	Bandwidth or EIP	1 minute

Metric	Meaning	Value Range	Monitored Object	Monitoring Period (Raw Data)
Inbound Bandwidth (originally named "Downstream Bandwidth")	Network rate of inbound traffic	≥ 0 bits/s	Bandwidth or EIP	1 minute
Outbound Bandwidth Usage	Usage of outbound bandwidth in percentage.	0-100%	Bandwidth or EIP	1 minute
Inbound Bandwidth Usage	Usage of inbound bandwidth in the unit of percent.	0-100%	Bandwidth or EIP	1 minute
Outbound Traffic (originally named "Upstream Traffic")	Network traffic going out of the cloud platform	≥ 0 bytes	Bandwidth or EIP	1 minute
Inbound Traffic (originally named "Downstream Traffic")	Network traffic going into the cloud platform	≥ 0 bytes	Bandwidth or EIP	1 minute

Viewing Load Balancer Traffic Metrics

1. Go to the [load balancer list page](#).
2. On the load balancer list page, locate the load balancer and click its name.
3. Click the **Monitoring** tab, select load balancer for **Dimension**, and view the graphs of inbound and outbound rates.

You can view data from the last 1, 3, 12 hours, last day, or the last 7 days.

1.12 Auditing

1.12.1 Key Operations Recorded by CTS

You can use CTS to record operations on ELB for query, auditing, and backtracking.

Table 1-79 lists the operations recorded by CTS.

Table 1-79 ELB operations recorded by CTS

Action	Resource Type	Trace Name
Configuring access logs	logtank	createLogtank
Deleting access logs	logtank	deleteLogtank
Creating a certificate	certificate	createCertificate
Modifying a certificate	certificate	updateCertificate
Deleting a certificate	certificate	deleteCertificate
Creating a health check	healthmonitor	createHealthMonitor
Modifying a health check	healthmonitor	updateHealthMonitor
Deleting a health check	healthmonitor	deleteHealthMonitor
Adding a forwarding policy	l7policy	createL7policy
Modifying a forwarding policy	l7policy	updateL7policy
Deleting a forwarding policy	l7policy	deleteL7policy
Adding a forwarding rule	l7rule	createL7rule
Modifying a forwarding rule	l7rule	updateL7rule
Deleting a forwarding rule	l7rule	deleteL7rule
Adding a listener	listener	createListener
Modifying a listener	listener	updateListener
Deleting a listener	listener	deleteListener
Creating a load balancer	loadbalancer	createLoadbalancer
Modifying a load balancer	loadbalancer	updateLoadbalancer
Deleting a load balancer	loadbalancer	deleteLoadbalancer


Action	Resource Type	Trace Name
Adding a backend server	member	createMember
Modifying a backend server	member	updateMember
Removing a backend server	member	batchUpdateMember
Creating a backend server group	pool	createPool
Modifying a backend server group	pool	updatPool
Deleting a backend server group	pool	deletePool

1.12.2 Viewing Traces

Scenarios

CTS records the operations performed on ELB and allows you to view the traces of the last seven days on the CTS console. To query these traces, perform the following operations.

Procedure

1. Log in to the management console.
2. In the upper left corner of the page, click  and select the desired region and project.
3. Under **Management & Governance**, click **Cloud Trace Service**.
4. In the navigation pane on the left, choose **Trace List**.
5. Specify the filters used for querying traces. The following filters are available:
 - **Trace Type, Trace Source, Resource Type, and Search By**
Select a filter from the drop-down list.
If you select **Trace name** for **Search By**, you need to select a specific trace name.
If you select **Resource ID** for **Search By**, select or enter a specific resource ID.
If you select **Resource name** for **Search By**, select or enter a specific resource name.
 - **Operator**: Select a specific operator (at the user level rather than the tenant level).
 - **Trace Status**: Available options include **All trace statuses, Normal, Warning, and Incident**. You can only select one of them.


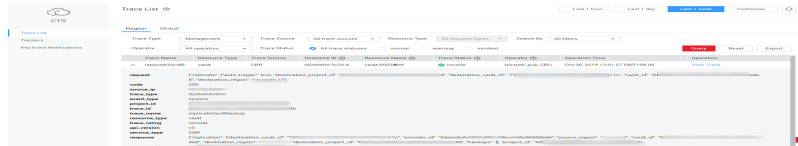
- Time range: You can query traces generated at any time range of the last seven days.
6. Click  on the left of the required trace to expand its details.

Figure 1-41 Expanding trace details



7. Click **View Trace** in the **Operation** column to view trace details.

Figure 1-42 View Trace



For details about key fields in the trace, see the [Cloud Trace Service User Guide](#).

Example Traces

- **Creating a load balancer**

```

request {"loadbalancer":{"name":"elb-test-zcy","description":"","tenant_id":"05041ffa40025702f6dc009cc6f8f33","vip_subnet_id":"ed04fd93-e74b-4794-b63e-e72baa02a2da","admin_state_up":true}}
code 201
source_ip 124.71.93.36
trace_type ConsoleAction
event_type system
project_id 05041ffa40025702f6dc009cc6f8f33
trace_id b39b21a1-8d49-11ec-b548-2be046112888
trace_name createLoadbalancer
resource_type loadbalancer
trace_rating normal
api_version v2.0
service_type ELB
response {"loadbalancer": {"description": "", "provisioning_status": "ACTIVE", "provider": "vlb", "project_id": "05041ffa40025702f6dc009cc6f8f33", "vip_address": "172.18.0.205", "pools": [], "operating_status": "ONLINE", "name": "elb-test-zcy", "created_at": "2022-02-14T03:53:39", "listeners": [], "id": "7ebe23cd-1d46-4a49-b707-1441c7f0d0d1", "vip_port_id": "5b36ff96-3773-4736-83cf-38c54abedeea", "updated_at": "2022-02-14T03:53:41", "tags": [], "admin_state_up": true, "vip_subnet_id": "ed04fd93-e74b-4794-b63e-e72baa02a2da", "tenant_id": "05041ffa40025702f6dc009cc6f8f33"}}
resource_id 7ebe23cd-1d46-4a49-b707-1441c7f0d0d1
tracker_name system
time 2022/02/14 11:53:42 GMT+08:00

```

```
resource_name elb-test-zcy
record_time 2022/02/14 11:53:42 GMT+08:00
request_id
user {"domain": {"name": "CBUInfo", "id": "0503dda87802345ddafed096d70a960"}, "name": "zcy", "id": "09f106afd2345cdeff5c009c58f5b4a"}
```

- Deleting a load balancer

```
request
code 204
source_ip 124.71.93.36
trace_type ConsoleAction
event_type system
project_id 05041fffa40025702f6dc009cc6f8f33
trace_id 4f838bbf-8d4a-11ec-a1fe-1f93fdaf3bec
trace_name deleteLoadbalancer
resource_type loadbalancer
trace_rating normal
api_version v2.0
service_type ELB
response {"loadbalancer": {"listeners": [], "vip_port_id": "5b36ff96-3773-4736-83cf-38c54abedeea", "tags": [], "tenant_id": "05041fffa40025702f6dc009cc6f8f33", "admin_state_up": true, "id": "7ebe23cd-1d46-4a49-b707-1441c7f0d0d1", "operating_status": "ONLINE", "description": "", "pools": [], "vip_subnet_id": "ed04fd93-e74b-4794-b63e-e72baa02a2da", "project_id": "05041fffa40025702f6dc009cc6f8f33", "provisioning_status": "ACTIVE", "name": "elb-test-zcy", "created_at": "2022-02-14T03:53:39", "vip_address": "172.18.0.205", "updated_at": "2022-02-14T03:53:41", "provider": "v1b"}}
resource_id 7ebe23cd-1d46-4a49-b707-1441c7f0d0d1
tracker_name system
time 2022/02/14 11:58:03 GMT+08:00
resource_name elb-test-zcy
record_time 2022/02/14 11:58:03 GMT+08:00
request_id
user {"domain": {"name": "CBUInfo", "id": "0503dda87802345ddafed096d70a960"}, "name": "zcy", "id": "09f106afd2345cdeff5c009c58f5b4a"}
```

2 User Guide for Shared Load Balancers

2.1 Permissions Management

2.1.1 Creating a User and Granting Permissions

Use [IAM](#) to implement fine-grained permissions control over your ELB resources. With IAM, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing ELB resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust another Huawei Cloud account or cloud service to perform efficient O&M on your ELB resources.

Skip this section if your Huawei Cloud account does not need individual IAM users.

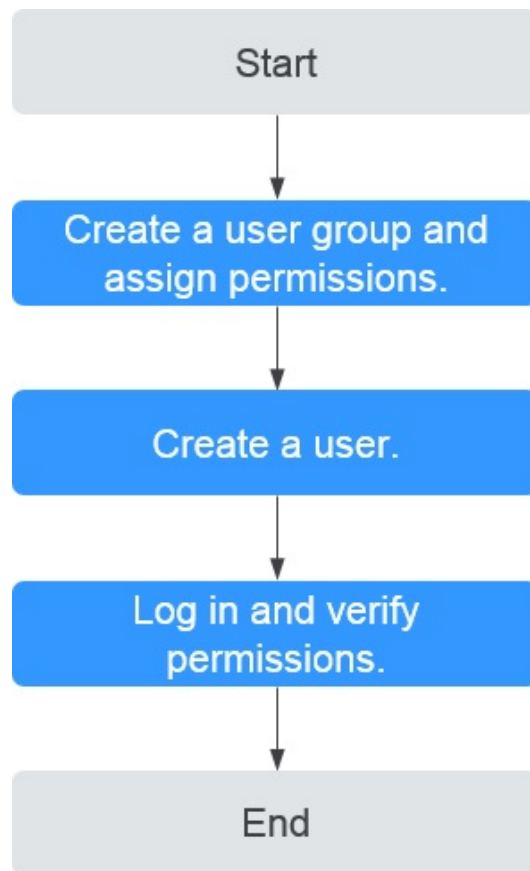
This following describes the procedure for granting permissions.

Prerequisites

You have learned about ELB policies and can select the appropriate policies based on service requirements. Learn about [permissions](#) supported by ELB. For the permissions of other services, see [System Permissions](#).

Process Flow

Figure 2-1 Process for granting ELB permissions



1. **Create a user group and assign permissions.**
Create a user group on the IAM console, and assign the **ELB ReadOnlyAccess** policy to the group.
2. **Create a user and add it to a user group.**
Create a user on the IAM console and add the user to the group created in 1.
3. **Log in** and verify permissions.
Log in to the ELB console by using the created user, and verify that the user only has read permissions for ELB.
 - Choose **Service List > Elastic Load Balance**. Then click **Buy Elastic Load Balancer** on the ELB console. If you cannot create a load balancer, the **ELB ReadOnlyAccess** policy has taken effect.
 - Choose any other service in **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the **ELB ReadOnlyAccess** policy has already taken effect.

2.1.2 Creating a Custom Policy

Custom policies can be created as a supplement to the system policies of ELB. For the actions supported for custom policies, see "Permissions Policies and Supported Actions" in the [Elastic Load Balance API Reference](#).

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Create a JSON policy or edit an existing one.

For details, see [Creating a Custom Policy](#). The following section contains examples of common ELB custom policies.

Example Custom Policies

- Example 1: Allowing users to update a load balancer

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "elb:loadbalancers:put"
      ]
    }
  ]
}
```

- Example 2: Denying load balancer deletion

A deny policy must be used in conjunction with other policies to take effect. If the permissions assigned to a user contain both Allow and Deny actions, the Deny actions take precedence over the Allow actions.

If you grant the system policy **ELB FullAccess** to a user but do not want the user to have the permission to delete load balancers defined in the policy, you can create a custom policy that rejects the deletion of load balancers and grant the **ELB FullAccess** and deny policies to the user, so that the user can perform all operations on ELB except deleting load balancers. The following is an example deny policy:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "elb:loadbalancers:delete"
      ]
    }
  ]
}
```

- Example 3: Defining permissions for multiple services in a policy

A custom policy can contain the actions of multiple services that are of the global or project-level type. The following is an example policy containing actions of multiple services:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "elb:loadbalancers:get",
        "elb:loadbalancers:list",
        "elb:loadbalancers:delete",
        "ecs:cloudServers:delete"
      ]
    }
  ]
}
```



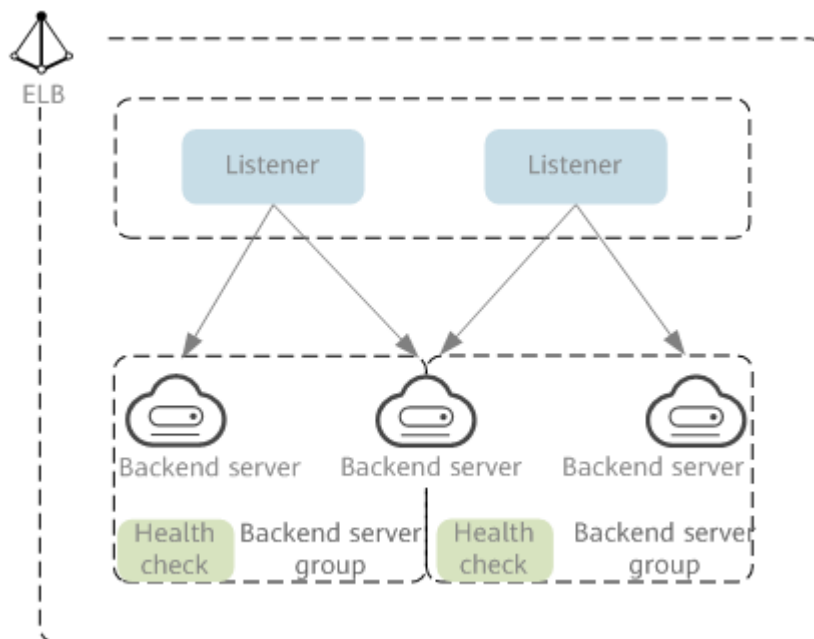
```
}  
]  
}
```

2.2 Load Balancer

2.2.1 Shared Load Balancer Overview

A load balancer distributes incoming traffic across multiple backend servers. Before using a load balancer, you need to add at least one listener to it and associate one backend server with it.

Figure 2-2 ELB components



Region

When you select a region, note the following:

- The region must be close to your users to reduce network latency and improve the download speed.
- Shared load balancers cannot distribute traffic across regions. When creating a load balancer, select the same region as the backend servers.

Network Type

Shared load balancers can work on both public and private networks.

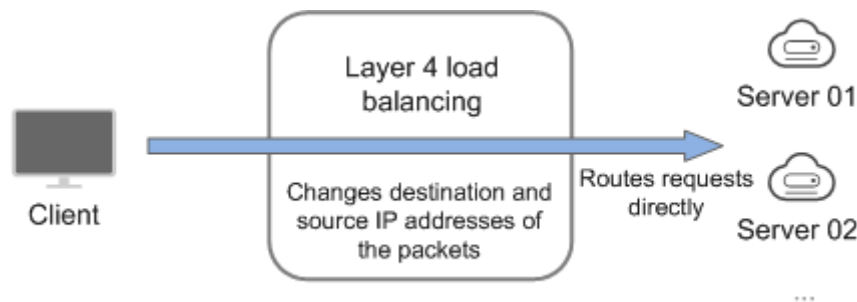
- To distribute requests over the Internet, you need to assign an EIP or bind an existing EIP to a load balancer so that it can route requests from the Internet to backend servers.
- If you want to distribute requests within a VPC, create a private network load balancer. This type of load balancers has only private IP addresses and can be only accessed within a VPC.

Protocol

ELB provides load balancing at both Layer 4 and Layer 7.

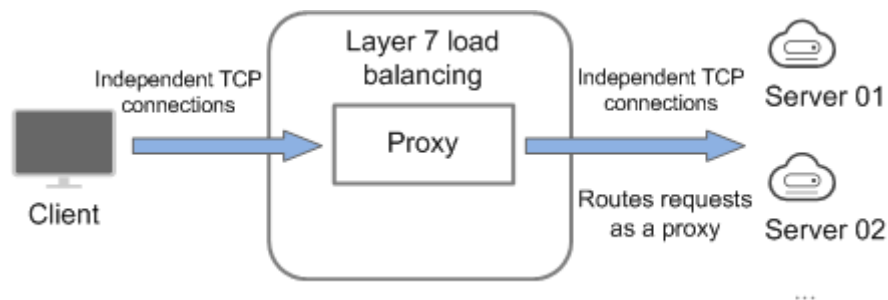
- If you choose TCP or UDP, the load balancer routes requests directly to backend servers. In this process, the destination IP address in a packet is changed to the IP address of the backend server, and the source IP address to the private IP address of the load balancer. A connection is established after a three-way handshake between the client and the backend server, and the load balancer only forwards the data.

Figure 2-3 Layer-4 load balancing



- Load balancing at Layer 7 is also called "content exchange". Once the load balancer receives a request, it works as a proxy for backend servers and initiates a connection (three-way handshake) with the client. It then determines which backend server to route the request to based on the fields in the HTTP/HTTPS request header and the load balancing algorithm you select when you add the listener.

Figure 2-4 Layer-7 load balancing



NOTE

ELB establishes persistent connections between the clients and the load balancers to reduce the costs of a large number of short connections. After a persistent connection is established, the client can keep sending HTTP or HTTPS requests to the load balancer until the connection times out.

Backend Server

Before you use ELB, you need to create cloud servers, deploy required applications on them, and add the cloud servers to one or more backend server groups. When you create cloud servers, note the following:

- Cloud servers should be in the same region as the load balancer.
- Cloud servers that run the same OS are recommended so that you can manage them more easily.
- ELB does not support File Transfer Protocol (FTP), but supports Secure File Transfer Protocol (SFTP) on backend servers.

2.2.2 Creating a Shared Load Balancer

Scenarios

You have prepared everything required for creating a shared load balancer. For details, see [Shared Load Balancer Overview](#).

Notes and Constraints

- After a load balancer is created, the VPC cannot be changed. If you want to change the VPC, create another load balancer and select a different VPC.
- To ping the IP address of a shared load balancer, you need to add a listener to it.

Procedure

1. Go to the [Buy Elastic Load Balancer](#) page.
2. On the load balancer list page, click **Buy Elastic Load Balancer**.
Complete the basic configurations based on [Table 2-1](#).

Table 2-1 Parameters for configuring the basic information

Parameter	Description
Type	Specifies the type of the shared load balancer. The type cannot be changed after the load balancer is created. Shared load balancers are suitable for workloads with low traffic, such as small websites and common HA applications. For details about the differences, see Differences Between Dedicated and Shared Load Balancers .
Billing Mode	Specifies the billing mode of the shared load balancer. You are charged for how long you use each load balancer.
Region	Specifies the desired region. Resources in different regions cannot communicate with each other over internal networks. For lower network latency and faster access to resources, select the nearest region.

Parameter	Description
Name	Specifies the load balancer name. The name can contain: <ul style="list-style-type: none">• 1 to 64 characters.• Letters, digits, underscores (_), hyphens (-), and periods (.).
Enterprise Project	Specifies an enterprise project by which cloud resources and members are centrally managed. For details about creating and managing enterprise projects, see the Enterprise Management User Guide .

3. Configure the network parameters based on [Table 2-2](#).

Table 2-2 Configuring network parameters

Parameter	Description
Network Type	Private IPv4 network is selected by default. The load balancer routes IPv4 requests from clients to backend servers in a VPC. If you want the load balancer to route requests from the Internet, bind an EIP to the load balancer.
VPC	Specifies the VPC where the shared load balancer works. You cannot change the VPC after the load balancer is created. Plan the VPC as required. Select an existing VPC, or click View VPCs to create a desired one. For more information about VPC, see the Virtual Private Cloud User Guide .
Frontend Subnet	Specifies the frontend subnet from which an IP address will be assigned to the shared load balancer to receive client requests. IP addresses in this subnet will be assigned to your load balancers.
IPv4 Address	Specifies how you want the IPv4 address to be assigned. <ul style="list-style-type: none">• Automatically assign IP address: The system assigns an IPv4 address to the load balancer.• Manually specify IP address: You need to manually specify an IPv4 address for the load balancer. NOTE Network ACL rules configured for the frontend subnet of a load balancer do not restrict traffic from clients to the load balancer. Use access control to limit which IP addresses can access the load balancer. For details, see What Is Access Control?

Parameter	Description
Guaranteed Performance	Specifies whether to enable the guaranteed performance option. This option allows your load balancers to handle up to 50,000 concurrent connections, 5,000 new connections per second, and 5,000 queries per second.

4. Configure an EIP for the load balancer to enable it to route IPv4 requests over the Internet based on [Table 2-3](#).

Table 2-3 Selecting an EIP for the load balancer

Parameter	Description
EIP	<p>Specifies the public IP address that will be bound to the load balancer for receiving and forwarding requests over the Internet.</p> <ul style="list-style-type: none">● Auto assign: A new EIP will be assigned to the load balancer.● Use existing: Select an existing EIP.● Not required: You can bind an EIP to the load balancer later.
EIP Type	<p>Specifies the link type (BGP) when a new EIP is used.</p> <ul style="list-style-type: none">● Dynamic BGP: When changes occur on a network using dynamic BGP, routing protocols provide automatic, real-time optimization of network configurations, ensuring network stability and optimal user experience. This option works well for workloads that require higher network stability and connectivity, such as financial transactions, online games, large-scale enterprise applications, and livestreaming services.● Static BGP: If there are changes on a network using static BGP, carriers cannot adjust network configurations in real time to ensure optimal user experience. This is a more cost-effective option that is a great fit for workloads that are running in relatively stable networks and have disaster recovery setups.● EIP Pool: assigns EIPs with dynamic BGP routing, ensuring network stability and optimal user experience. <p>For details see What Are the Differences Between Static BGP and Dynamic BGP?</p>

Parameter	Description
Billed By	Specifies how the bandwidth will be billed. You can select one from the following options: <ul style="list-style-type: none">● Bandwidth: You specify the maximum bandwidth and pay for the amount of time you use the bandwidth.● Traffic: You specify the maximum bandwidth and pay for the outbound traffic you use.● Shared Bandwidth: Load balancers that have EIPs bound in the same region can share the selected bandwidth, helping you reduce public network bandwidth costs.
Bandwidth (Mbit/s)	Specifies the maximum bandwidth.

5. Configure other parameters for the load balancer as described in [Table 2-4](#).

Table 2-4 Configuring other parameters



Parameter	Description
Advanced Settings (Optional) > Description	Click  to expand the configuration area and set this parameter. Enter a description about the load balancer in the text box as required. Enter up to 255 characters. Angle brackets (<>) are not allowed.
Advanced Settings (Optional) > Tag	Click  to expand the configuration area and set this parameter. Add tags to the load balancers so that they can be easily found. A tag consists of a tag key and a tag value. The tag key marks a tag, and the tag value specifies specific tag content. For details about the naming rules, see Table 2-5 . You can add a maximum of 20 tags.

Table 2-5 Tag naming rules



Parameter	Rule
Tag key	<ul style="list-style-type: none">• Cannot be empty.• Must be unique for the same load balancer.• Can contain a maximum of 36 characters.• Can contain only letters, digits, underscores (_), hyphens (-), at signs (@).
Tag value	<ul style="list-style-type: none">• Can contain a maximum of 43 characters.• Can contain only letters, digits, underscores (_), hyphens (-), at signs (@) are allowed.

6. Click **Buy Now**.

Exporting the Load Balancer List

You can export the information about all load balancers under your account to a local directory as an Excel file.

This file records the name, ID, status, type, and specifications of the load balancers.

1. Log in to the management console.
2. In the upper left corner of the page, click  and select the desired region and project.
3. Click  in the upper left corner to display **Service List** and choose **Networking > Elastic Load Balance**.
4. In the upper left corner of the load balancer list, click **Export**.

The system will export information about all of your load balancers as an Excel file to a local directory.

2.2.3 Configuring Modification Protection for Shared Load Balancers

You can enable modification protection for load balancers to prevent them from being modified or deleted by accident.

Procedure

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
3. Switch to the **Summary** tab and click **Configure** next to **Modification Protection**.
4. In the **Configure Modification Protection** dialog box, enable or disable **Modification Protection**.
Fill in the reason if needed.

 NOTE

You need to disable **Modification Protection** if you want to modify or delete a load balancer.

2.2.4 Changing the Network Configurations of a Shared Load Balancer

You can change the network configurations of a shared load balancer as needed.

Binding or Unbinding an IPv4 EIP

You can bind or unbind an IPv4 EIP to or from a shared load balancer as required.

 NOTE

Load balancers without IPv4 EIPs cannot route requests over the public IPv4 network.

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click **More** in the **Operation** column.
 - a. Binding an IPv4 EIP
 - i. Click **Bind IPv4 EIP**.
 - ii. In the **Bind IPv4 EIP** dialog box, select the EIP you want to bind to the load balancer and click **OK**.
 - b. Unbinding an IPv4 EIP
 - i. Click **Unbind IPv4 EIP**.
 - ii. In the displayed dialog box, confirm the IPv4 EIP that you want to unbind and click **OK**.

Modifying the Bandwidth

If you set the **Network Type** of a load balancer to **Public IPv4 network**, the load balancer can route requests over the Internet and you can modify the bandwidth used by the EIP bound to the load balancer as required. When you modify the bandwidth, traffic routing will not be interrupted.

 NOTE

The EIP bandwidth defines the limit for clients to access the load balancer.

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click **More** in the **Operation** column.
3. Click **Modify IPv4 Bandwidth**.
4. In the **New Configuration** area, modify the billing option and bandwidth and click **Next**.

You can select the bandwidth defined by the system or customize a bandwidth. The bandwidth ranges from 1 Mbit/s to 2,000 Mbit/s.
5. Confirm the new bandwidth and click **Submit**.

 NOTE

After you change the billing option and bandwidth, the price will be recalculated accordingly.

2.2.5 Deleting a Shared Load Balancer

Scenarios

You can delete a load balancer if you do not need it any longer.

 CAUTION

A deleted load balancer cannot be recovered.

After a public network load balancer is deleted, its EIP will not be released and can be used by other resources.

Notes and Constraints

- If **modification protection** is enabled for a load balancer, you need to disable modification protection on the **Summary** tab of the load balancer before deleting it.
- If **modification protection** is enabled for the listener added to a load balancer, you need to disable modification protection on the **Summary** tab of the listener before deleting the load balancer.
- If **modification protection** is enabled for the backend server group associated with the load balancer, you need to disable modification protection on the **Basic Information** area in the **Summary** tab of the backend server group before deleting the load balancer.

Deleting a Load Balancer

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the target load balancer and choose **More > Delete** in the **Operation** column.
A confirmation dialog box is displayed.
3. In the displayed dialog box, enter **DELETE**.
4. Click **OK**.

2.2.6 Enabling or Disabling a Shared Load Balancer

You can enable or disable a shared load balancer at any time. The load balancer stops receiving and routing traffic after it is disabled.

If some load balancers are not required but cannot be deleted, you can disable them.

Procedure

You can enable or disable a load balancer at any time. The load balancer stops receiving and routing traffic after it is disabled.

1. Go to the [load balancer list page](#).
2. Locate the load balancer and choose **More > Enable** or **More > Disable**.
3. Click **Yes**.

CAUTION

Disabled load balancers will still be billed.

2.2.7 Enabling Guaranteed Performance for a Shared Load Balancer

Scenarios

Guaranteed performance allows shared load balancers to handle up to 50,000 concurrent connections, 5,000 new connections per second, and 5,000 queries per second. It provides you with more stable and reliable load balancing capabilities in case of traffic surge.

If your shared load balancers were created after February 10, 2023, guaranteed performance will be enabled for them by default.

If your shared load balancers were created before February 10, 2023, perform the following operations to enable guaranteed performance.

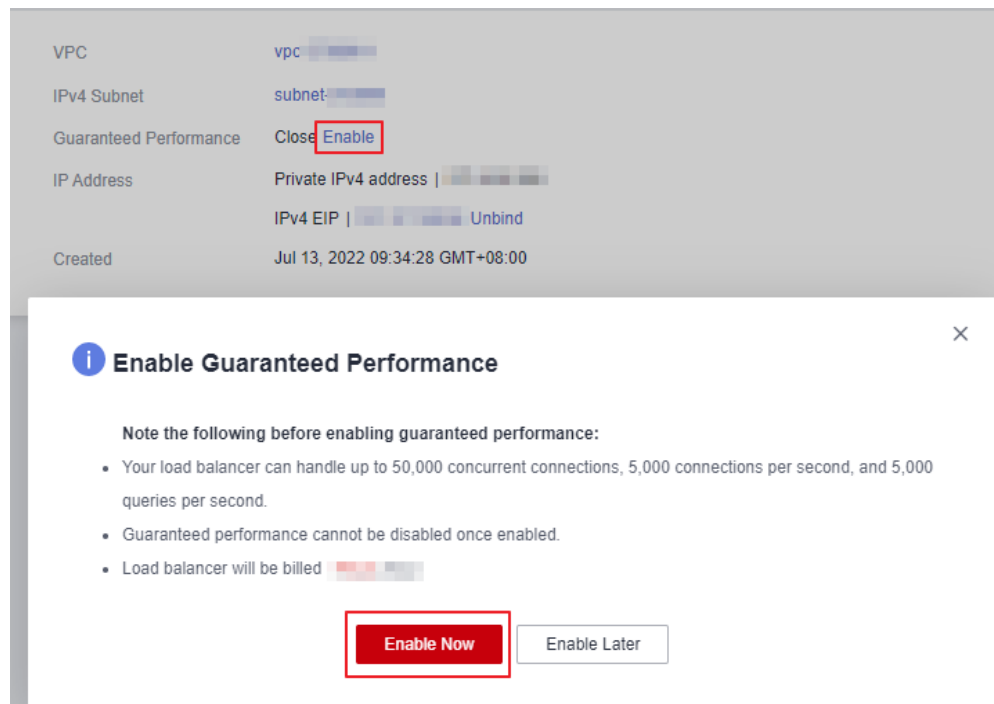
Notes

- Guaranteed performance cannot be disabled once enabled.
- After guaranteed performance is enabled, shared load balancers will be billed on a pay-per-use basis. For details about product prices, see [Product Pricing Details](#).

Procedure

1. Go to the [load balancer list page](#).
2. Locate the target shared load balancer and click its name to enter the **Summary** page.
3. Click **Enable**.
4. Click **Enable Now**.

Figure 2-5 Enabling guaranteed performance



2.3 Listener

2.3.1 Listener Overview

A listener checks requests from clients and routes requests to backend servers using the protocol, port, and load balancing algorithm you select. You need to add at least one listener after you have created a shared load balancer.

Supported Protocols

ELB provides load balancing at both Layer 4 and Layer 7. You can select TCP or UDP for load balancing at Layer 4 and HTTP or HTTPS for load balancing at Layer 7.

Table 2-6 Protocols supported by ELB

Protocol		Description	Scenario
Layer 4	TCP	<ul style="list-style-type: none"> Source IP address-based sticky sessions Fast data transfer 	<ul style="list-style-type: none"> Scenarios that require high reliability and data accuracy, such as file transfer, email, and remote login Web applications that receive a large number of concurrent requests and require high performance

Protocol		Description	Scenario
Layer 4	UDP	<ul style="list-style-type: none">• Relatively low reliability• Fast data transfer	Scenarios that require quick response, such as video chat, gaming, and real-time financial quotations
Layer 7	HTTP	<ul style="list-style-type: none">• Cookie-based sticky sessions• X-Forward-For request header	Web applications where data content needs to be identified, such as mobile games
Layer 7	HTTPS	<ul style="list-style-type: none">• An extension of HTTP for encrypted data transmission that can prevent unauthorized access• Encryption and decryption performed on load balancers• Multiple versions of encryption protocols and cipher suites	Web applications that require encrypted transmission

Frontend Protocols and Ports

Frontend protocols and ports are used by load balancers to receive requests from clients. Load balancers use TCP or UDP at Layer 4, and HTTP or HTTPS at Layer 7. Select a protocol and a port that best suit your requirements.

NOTE

The frontend protocols and ports cannot be changed once a listener is added. If you want to use a different protocol and port, add another listener.

Table 2-7 Frontend protocols and ports

Frontend Protocol	TCP, UDP, HTTP, and HTTPS
-------------------	---------------------------

Frontend Port	Listeners using different protocols of a load balancer cannot use the same port. However, UDP listeners can use the same port as listeners that use other protocols. For example, if there is a UDP listener that uses port 88, you can add a TCP listener that also uses port 88. The port number ranges from 1 to 65535. The following are some commonly-used protocols and port numbers: TCP/80 HTTPS/443
----------------------	---

Backend Protocols and Ports

Backend protocols and ports are used by backend servers to receive requests from load balancers. If Windows servers have Internet Information Services (IIS) installed, the default backend protocol and port are HTTP and 80.

Table 2-8 Backend protocols and ports

Backend Protocol	TCP, UDP, and HTTP
Backend Port	Backend servers of a load balancer can use the same ports. The port number ranges from 1 to 65535. The following are some commonly-used protocols and port numbers: TCP/80 HTTP/443

2.3.2 Adding a TCP Listener

Scenarios

You can add a TCP listener, if high reliability and high accuracy are required but slow speed is acceptable. TCP works well for applications such as file transfer, email sending and receiving, and remote login.

Notes and Constraints

If the front protocol is TCP, the backend protocol defaults to TCP and cannot be changed.

Procedure

1. Go to the [load balancer list page](#).

2. On the displayed page, locate the load balancer and click its name.
3. Under **Listeners**, click **Add Listener**. Configure the parameters based on [Table 2-9](#).

Table 2-9 Parameters for configuring a TCP listener

Parameter	Description
Name	Specifies the listener name.
Frontend Protocol	Specifies the protocol that will be used by the load balancer to receive requests from clients. Select TCP .
Frontend Port	Specifies the port that will be used by the load balancer to receive requests from clients. The port number ranges from 1 to 65535.
Access Control	Specifies how access to the listener is controlled. For details, see What Is Access Control? The following options are available: <ul style="list-style-type: none">• All IP addresses• Blacklist• Whitelist
IP Address Group	Specifies the IP address group associated with a whitelist or blacklist. If there is no IP address group, create one first. For more information, see IP Address Group .
Transfer Client IP Address	Specifies whether to transmit IP addresses of the clients to backend servers.
Advanced Settings	
Idle Timeout (s)	Specifies the length of time for a connection to keep alive, in seconds. If no request is received within this period, the load balancer closes the connection and establishes a new one with the client when the next request arrives. The idle timeout duration ranges from 10 to 4000 .
Tag	Adds tags to the listener. Each tag is a key-value pair, and the tag key is unique.
Description	Provides supplementary information about the listener. You can enter a maximum of 255 characters.

4. Click **Next: Configure Request Routing Policy**.
 - a. You are advised to select an existing backend server group.
 - b. You can also click **Create new** to create a backend server group.

- i. Configure the backend server group based on [Table 2-21](#).
- ii. Click **Next: Add Backend Server**. Add backend servers and configure health check for the backend server group.

For details about how to add backend servers, see [Backend Server Overview](#). For the parameters required for configuring a health check, see [Table 2-22](#).

5. Click **Next: Confirm**.
6. Confirm the configurations and click **Submit**.

2.3.3 Adding a UDP Listener

Scenarios

You can add a UDP listener, if quick response is required but low reliability is acceptable. UDP listeners are suitable for scenarios such as video chat, gaming, and real-time financial quotations.

Notes and Constraints

- UDP listeners do not support fragmentation.
- The port of UDP listeners cannot be 4789.
- UDP packets can have any size less than 1,500 bytes. The packets will be discarded if they are bigger than 1,500 bytes. To avoid this, you need to modify the configuration files of the applications based on the maximum transmission unit (MTU) value.
- If the listener protocol is UDP, the protocol of the backend server group is UDP by default and cannot be changed.

Procedure

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
3. Under **Listeners**, click **Add Listener**. Configure the parameters based on [Table 2-10](#).

Table 2-10 Parameters for configuring a UDP listener

Parameter	Description
Name	Specifies the listener name.
Frontend Protocol	Specifies the protocol that will be used by the load balancer to receive requests from clients. Select UDP .
Frontend Port	Specifies the port that will be used by the load balancer to receive requests from clients. The port number ranges from 1 to 65535.

Parameter	Description
Access Control	Specifies how access to the listener is controlled. For details, see What Is Access Control? The following options are available: <ul style="list-style-type: none">• All IP addresses• Blacklist• Whitelist
IP Address Group	Specifies the IP address group associated with a whitelist or blacklist. If there is no IP address group, create one first. For more information, see IP Address Group .
Transfer Client IP Address	Specifies whether to transmit IP addresses of the clients to backend servers.
Advanced Settings	
Tag	Adds tags to the listener. Each tag is a key-value pair, and the tag key is unique.
Description	Provides supplementary information about the listener. You can enter a maximum of 255 characters.

4. Click **Next: Configure Request Routing Policy**.
 - a. You are advised to select an existing backend server group.
 - b. You can also click **Create new** to create a backend server group.
 - i. Configure the backend server group based on [Table 2-21](#).
 - ii. Click **Next: Add Backend Server**. Add backend servers and configure health check for the backend server group.
For details about how to add backend servers, see [Backend Server Overview](#). For the parameters required for configuring a health check, see [Table 2-22](#).
5. Click **Next: Confirm**.
6. Confirm the configurations and click **Submit**.

2.3.4 Adding an HTTP Listener

Scenarios

You can add an HTTP listener if content identification is required. HTTP is a great fit for workloads such as web applications and mobile mini-games.

Notes and Constraints

If the listener protocol is HTTP, the backend protocol is HTTP by default and cannot be changed.

Procedure

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
3. Under **Listeners**, click **Add Listener**. Configure the parameters based on [Table 2-11](#).

Table 2-11 Parameters for configuring an HTTP listener

Parameter	Description
Name	Specifies the listener name.
Frontend Protocol	Specifies the protocol that will be used by the load balancer to receive requests from clients. Select HTTP .
Frontend Port	Specifies the port that will be used by the load balancer to receive requests from clients. The port number ranges from 1 to 65535.
Redirect	Specifies whether to enable redirection. If you have both HTTPS and HTTP listeners, you can use this function to redirect the requests from the HTTP listener to the HTTPS listener to ensure security. After the redirection is added for an HTTP listener, the backend server will return 301 Moved Permanently to the clients.
Redirected To	Select the HTTPS listener to which requests are redirected.
Access Control	Specifies how access to the listener is controlled. For details, see What Is Access Control? The following options are available: <ul style="list-style-type: none">• All IP addresses• Blacklist• Whitelist
IP Address Group	Specifies the IP address group associated with a whitelist or blacklist. If there is no IP address group, create one first. For more information, see IP Address Group .
Transfer Client IP Address	Specifies whether to transmit IP addresses of the clients to backend servers.
Advanced Settings	

Parameter	Description
Transfer Load Balancer EIP	<p>Specifies whether to store the EIP bound to the load balancer in the X-Forwarded-ELB-IP header field and pass this field to backend servers.</p> <p>Enable this option if you want to transparently transmit the EIP of the load balancer to backend servers.</p>
Idle Timeout (s)	<p>Specifies the length of time for a connection to keep alive, in seconds. If no request is received within this period, the load balancer closes the connection and establishes a new one with the client when the next request arrives.</p> <p>The idle timeout duration ranges from 0 to 4000.</p>
Request Timeout (s)	<p>Specifies the length of time that a load balancer is willing to wait for a client request to complete. The load balancer terminates the connection if a request takes too long to complete.</p> <p>The request timeout duration ranges from 1 to 300.</p>
Response Timeout (s)	<p>Specifies the length of time (in seconds) after which the load balancer sends a 504 Gateway Timeout error to the client if the load balancer receives no response from the backend server after routing a request to the backend server and receives no response after attempting to route the same request to other backend servers.</p> <p>The response timeout duration ranges from 1 to 300.</p> <p>NOTE If you have enabled sticky sessions and the backend server does not respond within the response timeout duration, the load balancer returns 504 Gateway Timeout to the clients.</p>
Tag	<p>Adds tags to the listener. Each tag is a key-value pair, and the tag key is unique.</p>
Description	<p>Provides supplementary information about the listener.</p> <p>You can enter a maximum of 255 characters.</p>

4. Click **Next: Configure Request Routing Policy**.
 - a. You are advised to select an existing backend server group.
 - b. You can also click **Create new** to create a backend server group.
 - i. Configure the backend server group based on [Table 2-21](#).
 - ii. Click **Next: Add Backend Server**. Add backend servers and configure health check for the backend server group.

For details about how to add backend servers, see [Backend Server Overview](#). For the parameters required for configuring a health check, see [Table 2-22](#).

5. Click **Next: Confirm**.
6. Confirm the configurations and click **Submit**.

2.3.5 Adding an HTTPS Listener

Scenarios

You can add an HTTPS listener if you require encrypted transmission. Load balancers decrypt HTTPS requests before routing them to backend servers. Once the servers process the requests, they send them back to the load balancers for encryption. Finally, the load balancers send the encrypted requests to the clients.

When you add an HTTPS listener, ensure that the subnet of the load balancer has sufficient IP addresses. If the IP addresses are insufficient, add more subnets on the summary page of the load balancer. After you select a subnet, ensure that ACL rules are not configured for this subnet. If rules are configured, request packets may not be allowed.

Notes and Constraints

If the listener protocol is HTTPS, the protocol of the backend server group is HTTP by default and cannot be changed.

Procedure

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
3. Under **Listeners**, click **Add Listener**. Configure the parameters based on [Table 2-12](#).

Table 2-12 Parameters for configuring an HTTPS listener

Parameter	Description
Name	Specifies the listener name.
Frontend Protocol	Specifies the protocol that will be used by the load balancer to receive requests from clients. Select HTTPS .
Frontend Port	Specifies the port that will be used by the load balancer to receive requests from clients. The port number ranges from 1 to 65535.

Parameter	Description
SSL Authentication	<p>Specifies how you want the clients and backend servers to be authenticated.</p> <p>There are two options: One-way authentication or Mutual authentication.</p> <ul style="list-style-type: none">• If only server authentication is required, select One-way authentication.• If you want the clients and the load balancer to authenticate each other, select Mutual authentication. Only authenticated clients will be allowed to access the load balancer.
CA Certificate	<p>Specifies the certificate that allows the clients and backend servers to mutually authenticate each other.</p> <p>For details, see Adding a Certificate.</p>
Server Certificate	<p>Specifies the certificate that will be used by the backend server to authenticate the client when HTTPS is used as the frontend protocol.</p> <p>Both the certificate and private key are required.</p> <p>For details, see Adding a Certificate.</p>
Enable SNI	<p>Specifies whether to enable SNI when HTTPS is used as the frontend protocol.</p> <p>SNI is an extension to TLS and is used when a server uses multiple domain names and certificates.</p> <p>This allows the client to submit the domain name information while sending an SSL handshake request. After the load balancer receives the request, the load balancer queries the corresponding certificate based on the domain name and returns it to the client. If no certificate is found, the load balancer will return the default certificate. For details, see SNI Certificate.</p>
SNI Certificate	<p>Specifies the certificate associated with the domain name when the frontend protocol is HTTPS and SNI is enabled.</p> <p>Select an existing certificate or create one.</p> <p>For details, see Adding a Certificate.</p>
Access Control	<p>Specifies how access to the listener is controlled. For details, see What Is Access Control? The following options are available:</p> <ul style="list-style-type: none">• All IP addresses• Blacklist• Whitelist

Parameter	Description
IP Address Group	Specifies the IP address group associated with a whitelist or blacklist. If there is no IP address group, create one first. For more information, see IP Address Group .
Transfer Client IP Address	Specifies whether to transmit IP addresses of the clients to backend servers.
Advanced Settings	
Security Policy	Specifies the security policy you can use if you select HTTPS as the frontend protocol. For more information, see TLS Security Policy .
HTTP/2	Specifies whether you want to use HTTP/2 if you select HTTPS for Frontend Protocol . For details, see HTTP/2 .
Transfer Load Balancer EIP	Specifies whether to store the EIP bound to the load balancer in the X-Forwarded-ELB-IP header field and pass this field to backend servers. Enable this option if you want to transparently transmit the EIP of the load balancer to backend servers.
Idle Timeout (s)	Specifies the length of time for a connection to keep alive, in seconds. If no request is received within this period, the load balancer closes the connection and establishes a new one with the client when the next request arrives. The idle timeout duration ranges from 0 to 4000 .
Request Timeout (s)	Specifies the length of time that a load balancer is willing to wait for a client request to complete. The load balancer terminates the connection if a request takes too long to complete. The request timeout duration ranges from 1 to 300 .
Response Timeout (s)	Specifies the length of time (in seconds) after which the load balancer sends a 504 Gateway Timeout error to the client if the load balancer receives no response from the backend server after routing a request to the backend server and receives no response after attempting to route the same request to other backend servers. The response timeout duration ranges from 1 to 300 . NOTE If you have enabled sticky sessions and the backend server does not respond within the response timeout duration, the load balancer returns 504 Gateway Timeout to the clients.

Parameter	Description
Tag	Adds tags to the listener. Each tag is a key-value pair, and the tag key is unique.
Description	Provides supplementary information about the listener. You can enter a maximum of 255 characters.

4. Click **Next: Configure Request Routing Policy**.
 - a. You are advised to select an existing backend server group.
 - b. You can also click **Create new** to create a backend server group.
 - i. Configure the backend server group based on [Table 2-21](#).
 - ii. Click **Next: Add Backend Server**. Add backend servers and configure health check for the backend server group.
For details about how to add backend servers, see [Backend Server Overview](#). For the parameters required for configuring a health check, see [Table 2-22](#).
5. Click **Next: Confirm**.
6. Confirm the configurations and click **Submit**.

2.3.6 Forwarding Policy

Scenarios

You can configure forwarding policies for HTTP or HTTPS listeners to forward requests to different backend server groups based on domain names or paths.

This is suitable when requests of services such as videos, images, audios, and texts need to be forwarded to different backend servers.

A forwarding policy consists of two parts: forwarding rule and action.

- A forwarding rule can be a domain name or a path.
- HTTP listeners can forward requests to a backend server group or redirect requests to another listener.
- HTTPS listeners can forward requests to a backend server group.

How Requests Are Matched

- After receiving a request, the load balancer attempts to find a matching forwarding policy based on the domain name or URL in the request:
 - If a match is found, the request is forwarded to the backend server group you select or create when you add the forwarding policy.
 - If no match is found, the request is forwarded to the default backend server group (that is specified when the listener is created).
 - If both a domain name and path are configured for a forwarding policy, the request can match the forwarding policy only when the domain name and path are both met.

- Matching priority:
 - When a request matches both a domain name-based policy and a path-based policy, the domain named-based policy is matched first. [Table 2-13](#) shows an example.
 - Forwarding policy priorities are independent of each other regardless of domain names.
 - Path-based forwarding rules are applied in the following order of priority: an exact match rule, a prefix match rule, and a regular expression match rule. For multiple matches of the same type, only the longest path rule will be applied.

Table 2-13 Example forwarding policies

Request	Forwarding Policy	Forwarding Rule	Specified Value
www.elb.com/ test	1	Path	/test
	2	Domain name	www.elb.com

 **NOTE**

In this example, although request **www.elb.com/test** matches both forwarding policies, it is routed based on forwarding policy 2 because domain named-based forwarding rules are applied first.

Notes and Constraints

- Forwarding policies can be configured only for HTTP and HTTPS listeners.
- Forwarding policies must be unique.
- A maximum of 100 forwarding policies can be configured for a listener. If the number of forwarding policies exceeds the quota, the excess forwarding policies will not be applied.
- When you add a forwarding policy, note the following:
 - The path in a forwarding rule cannot contain query strings. For example, if the path is set to **/path/resource?name=value**, the forwarding policy is invalid.
 - Each path must exist on the backend server. If the path does not exist, the backend server will return 404 Not Found.
 - In the regular expression match, the characters are matched sequentially, and the matching ends when any rule is matched. Matching rules cannot overlap with each other.
 - A path cannot be configured for two forwarding policies.
 - A domain name cannot exceed 100 characters.

CAUTION

If you add a forwarding policy that is the same as an existing one by calling an API, there will be a conflict. Even if you delete the existing forwarding policy, the new forwarding policy is still unavailable. Delete the newly-added forwarding policy and add a different one.

Adding a Forwarding Policy

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer you want to add forwarding policies for and click its name.
3. On the **Listeners** tab, add a forwarding policy in either of the following ways:
 - Locate the target listener and click **Add/Edit Forwarding Policy** in the **Forwarding Policies** column.
 - Locate the target listener, click its name, and click the **Forwarding Policies** tab.
4. Click **Add Forwarding Policy**. Configure the parameters based on [Table 2-14](#).
5. After the configuration is complete, click **Save**.

Table 2-14 Forwarding policy parameters

Parameter		Description	Example Value
Forwarding Rule	Domain name	Specifies the domain name that will be exactly matched against the domain names in requests. You need to specify either a domain name or path.	www.test.com

Parameter		Description	Example Value
	Path	<ul style="list-style-type: none"> • Description Specifies the path used for forwarding requests. A path can contain letters, digits, and special characters: _~';@^-%#\$.*+?,=!: \/()[]{} • Matching rules <ul style="list-style-type: none"> - Exact match: The request path is the same as the specified path and must start with a slash (/). - Prefix match: The request path starts with the specified path and must start with a slash (/). - Regular expression match: The paths are matched using a regular expression. 	/login.php
Action	Forward to a backend server group	Specifies the backend server group to which a request is routed if it matches the configured forwarding rule.	Forward to a backend server group

Parameter		Description	Example Value
	Redirect to another listener	<p>Specifies the HTTPS listener to which a request is routed if it matches the configured forwarding rule.</p> <p>This action can be configured only for HTTP listeners.</p> <p>NOTE</p> <p>If you select Redirect to another listener, the HTTP listener will redirect requests to the specified HTTPS listener, but access control configured for the HTTP listener still takes effect.</p> <p>For example, if you configure a redirect for an HTTP listener, HTTP requests to access a web page will be redirected to the HTTPS listener you select and handled by the backend servers associated with the HTTPS listener. As a result, the clients access the web page over HTTPS. The configuration of the HTTP listener will become invalid.</p>	N/A
	Backend Server Group	<p>Select a backend server group that will receive requests from the load balancer.</p> <p>This parameter is mandatory when you set Action to Forward to a backend server group.</p>	N/A
	Listener	<p>Select an HTTPS listener that will receive requests redirected from the current HTTP listener.</p> <p>This parameter is mandatory when Action is set to Redirect to another listener.</p>	N/A

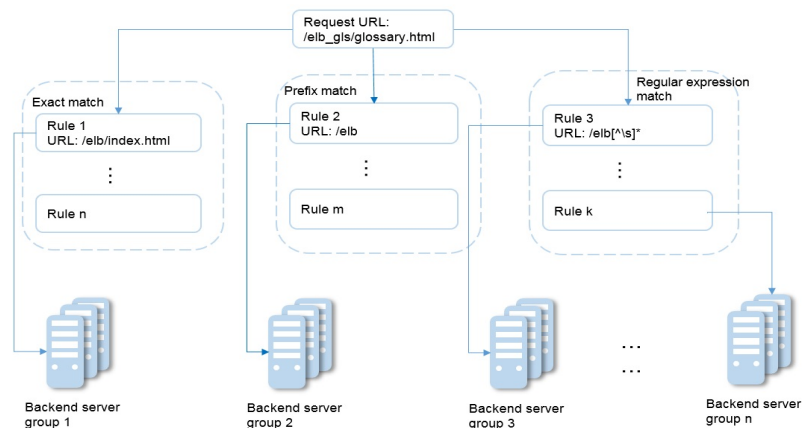
Path Matching Examples

The following table lists how a path is matched, and [Figure 2-6](#) shows how a request is forwarded to a backend server group.

Table 2-15 Path matching examples

URL Matching Rule	URL in the Request	Specified Path			
		/elb/index.html	/elb	/elb[^\s]*	/index.html
N/A	N/A				
Exact match	/elb/index.html	√	N/A	N/A	N/A
Prefix match		√	√	N/A	N/A
Regular expression match		√	N/A	√	N/A

Figure 2-6 Request forwarding



In this figure, the system first searches for an exact match of the request URL (/elb_gls/glossary.html). If there is no exact match, the system searches for a prefix match. If a match is found, the request is forwarded to backend server group 2 even if a regular expression match is also found, because the prefix match has a higher priority.

Modifying a Forwarding Policy

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer whose forwarding policies you want to modify and click its name.
3. Click **Listeners**, locate the listener, and click its name.
4. On the **Forwarding Policies** tab, select the forwarding policy, and click **Edit**.
5. Modify the parameters and click **Save**.

Deleting a Forwarding Policy

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer whose forwarding policies you want to delete and click its name.
3. Click **Listeners**, locate the listener, and click its name.
4. On the **Forwarding Policies** tab, select the forwarding policy, and click **Delete** on the top right.
5. In the displayed dialog box, click **OK**.

2.3.7 HTTP/2

What Is HTTP/2?

Hypertext Transfer Protocol 2.0 (HTTP/2) uses a binary format for data transmission. It allows for much faster transmission and multiplexing. To reduce latency and improve efficiency, you can enable HTTP/2 when you add HTTPS listeners.

Notes and Constraints

You can enable HTTP/2 only for HTTPS listeners.

Managing HTTP/2

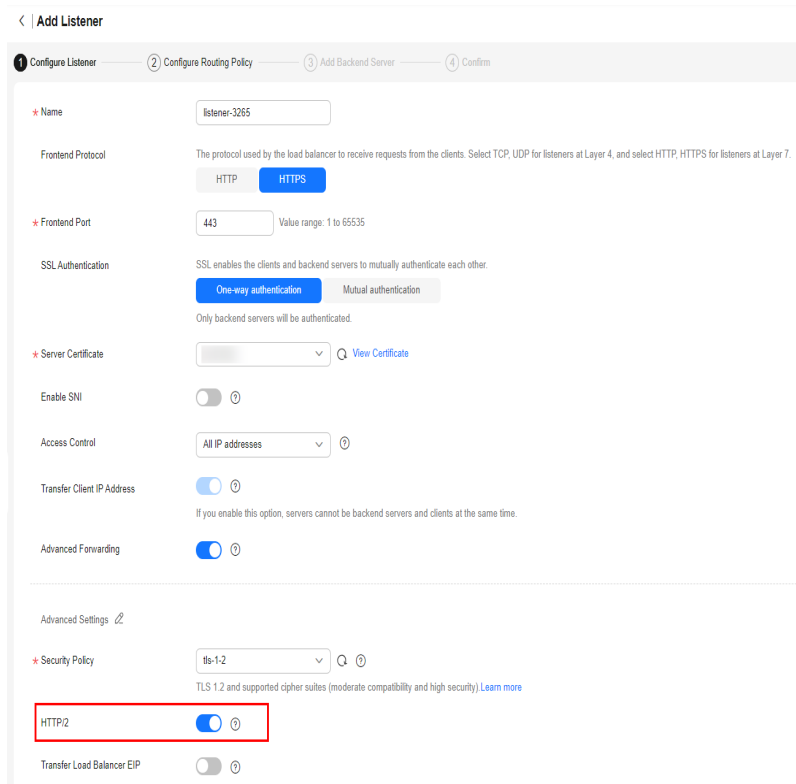
You can enable HTTP/2 when you add an HTTPS listener. You can enable or disable HTTP/2 for an existing HTTPS listener.

Enabling HTTP/2 When Adding a Listener

To enable HTTP/2 when adding an HTTPS listener, perform the following operations:

1. Go to the [load balancer list page](#).
2. Locate the load balancer and click its name.
3. Under **Listeners**, click **Add Listener**.
4. In the **Add Listener** dialog box, set **Frontend Protocol** to **HTTPS**.
5. Expand **Advanced Settings** and enable HTTP/2.
6. Confirm the configurations and go to the next step.

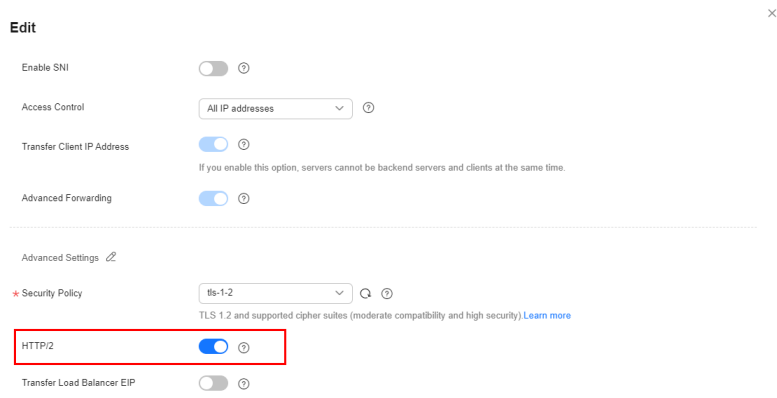
Figure 2-7 Enabling HTTP/2



Enabling or Disabling HTTP/2 for an Existing Listener

1. Go to the [load balancer list page](#).
2. Locate the load balancer and click its name.
3. Click **Listeners**, locate the listener, and click its name.
4. On the **Summary** tab, click **Edit** on the top right.
5. In the **Edit** dialog box, expand **Advanced Settings** and enable or disable HTTP/2.
6. Click **OK**.

Figure 2-8 Disabling or enabling HTTP/2



2.3.8 Modifying a Listener

Scenarios

You can configure modification protection for a listener, modify the settings of a listener, and change the backend server group of a listener as needed.

Prerequisites

- You have created a load balancer by referring to [Creating a Shared Load Balancer](#).
- You have created a backend server group by referring to [Creating a Backend Server Group](#).
- You have added a listener by referring to [Listener Overview](#).

Configuring Modification Protection for a Listener

You can enable modification protection for a listener to prevent it from being modified or deleted by accident.

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
3. Click **Listeners** tab, locate the listener, and click its name.
4. On the **Summary** tab, click **Configure** next to **Modification Protection**.
5. In the **Configure Modification Protection** dialog box, enable **Modification Protection**.

NOTE

You need to disable **Modification Protection** if you want to modify or delete a listener.

Modifying Listener Settings

NOTE

Frontend Protocol/Port and **Backend Protocol** cannot be modified. If you want to modify the protocol or port of the listener, add another listener to the load balancer.

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
3. Modify the listener in either of the following ways:
 - On the **Listeners** tab, locate the listener, and click **Edit** in the **Operation** column.
 - Click the name of the target listener. On the **Summary** tab, click **Edit** on the top right corner.
4. On the **Edit** page, modify parameters, and click **OK**.

Modifying Timeout Durations

You can modify timeout durations (idle timeout, request timeout, and response timeout) for your listeners to meet varied demands. For example, if the size of a

request from an HTTP or HTTPS client is large, you can prolong the request timeout duration to ensure that the request can be successfully routed.

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
3. Click **Listeners**, locate the listener, and click the name of the listener.
4. On the **Summary** tab, click **Edit** on the top right.
5. In the **Edit** dialog box, expand **Advanced Settings**.
6. Configure **Idle Timeout (s)**, **Request Timeout (s)**, or **Response Timeout (s)** as you need.
7. Click **OK**.

Changing the Backend Server Group of a Listener

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
3. On the **Listeners** tab, locate the target listener and click its name.
4. On the **Summary** tab, click **Change Backend Server Group** on the right of **Default Backend Server Group** area.
5. In the displayed dialog box, click the server group name box.
Select a backend server group from the drop-down list or create a group.
 - a. Click the name of the backend server group or enter the name in the search box to search for the target group.
 - b. Click **Create Backend Server Group**. After the backend server group is created, click the refresh icon.

NOTE

The backend protocol of the new backend server group must match the frontend protocol of the listener.

6. Click **OK**.

2.3.9 Deleting a Listener

Scenarios

You can modify a listener as needed or delete a listener if you no longer need it.

Deleted listeners cannot be recovered.

Notes and Constraints

If modification protection is enabled for a listener, the listener cannot be deleted or modified.

Procedure

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.

3. Click the **Listeners** tab, locate the listener, and click **Delete** in the **Operation** column.
4. In the displayed dialog box, enter **DELETE**.
5. Click **OK**.

2.4 Backend Server Group

2.4.1 Backend Server Group Overview

What Is a Backend Server Group?

A backend server group is a logical collection of one or more backend servers to receive massive concurrent requests at the same time. Only cloud servers can be added as backend servers.

The following table describes how a backend server group forwards traffic.

Table 2-16 Traffic distribution process

Step 1	A client sends a request to your application. The listeners added to your load balancer use the protocols and ports you have configured to forward the request to the associated backend server group.
Step 2	Healthy backend servers in the backend server group receive the request based on the load balancing algorithm, handle the request, and return a result to the client.
Step 3	In this way, massive concurrent requests can be processed at the same time, improving the availability of your applications.

Shared load balancers have only one type of backend server group, where you can only add cloud servers.

Table 2-17 Adding backend servers

Backend Server Type	Description	Reference
Cloud servers	You can add ECSs and BMSs that are in the same VPC as the load balancer.	Cloud Servers

Advantages

Backend server groups can bring the following benefits:

- **Reduced costs and easier management:** You can add or remove backend servers as traffic changes over the time. This can help avoid low resource utilization and makes it easy to manage backend servers.
- **Higher reliability:** Traffic is routed only to healthy backend servers in the backend server group.

Controlling Traffic Distribution

You can configure the key functions listed in [Table 2-18](#) for each backend server group to ensure service stability.

Table 2-18 Key functions

Key Function	Description	Detail
Load Balancing Algorithm	The load balancer distributes traffic based on the load balancing algorithm you have configured for the backend server group.	Load Balancing Algorithms
Sticky Session	Specifies whether to enable the sticky session option. If you enable this option, all requests from a client during one session are sent to the same backend server.	Sticky Session

Backend Server Group and Listener Protocols

A backend server group can be associated with only one shared load balancer and used by only one listener.

The backend protocol of the new backend server group must match the frontend protocol of the listener as described in [Table 2-19](#).

Table 2-19 The frontend and backend protocol

Frontend Protocol	Backend Protocol
TCP	TCP
UDP	UDP
HTTP	HTTP
HTTPS	HTTP

2.4.2 Creating a Backend Server Group

Scenario

To route requests, you need to associate a backend server group to each listener.

You can create a backend server group in the ways listed in [Table 2-20](#).

Table 2-20 Creating a backend server group

Scenario	Procedure
Creating a backend server group and associating it with a load balancer	Procedure
Creating a backend server group when adding a listener	You can add listeners using different protocols as required. For details, see Listener Overview . References are as follows: <ul style="list-style-type: none">• Adding a TCP Listener• Adding a UDP Listener• Adding an HTTP Listener• Adding an HTTPS Listener
Changing the backend server group associated with the listener	Changing a Backend Server Group

Notes and Constraints

The backend server group of a shared load balancer can be associated with only one listener.

Procedure

1. Go to the [backend server group list page](#).
2. Click **Create Backend Server Group** in the upper right corner.
3. Configure the routing policy based on [Table 2-21](#).

Table 2-21 Parameters required for configuring a routing policy


Parameter	Description
Load Balancer Type	Specifies the type of load balancers that can use the backend server group. Select Shared .
Load Balancer	Specifies whether to associate a load balancer.
Backend Server Group Name	Specifies the name of the backend server group.
Backend Protocol	Specifies the protocol that backend servers in the backend server group use to receive requests from the listeners. The protocol varies depending on the forwarding mode: The options are HTTP, TCP, and UDP.

Parameter	Description
Load Balancing Algorithm	<p>Specifies the algorithm used by the load balancer to distribute traffic. The following options are available:</p> <ul style="list-style-type: none">• Weighted round robin: Requests are routed to different servers based on their weights. Backend servers with higher weights receive proportionately more requests, whereas equal-weighted servers receive the same number of requests.• Weighted least connections: In addition to the number of connections, each server is assigned a weight based on its capacity. Requests are routed to the server with the lowest connections-to-weight ratio.• Source IP hash: Allows requests from different clients to be routed based on source IP addresses and ensures that requests from the same client are forwarded to the same server. <p>For more information about load balancing algorithms, see Load Balancing Algorithms.</p>
Sticky Session	<p>Specifies whether to enable sticky sessions. If you enable sticky sessions, all requests from the same client during one session are sent to the same backend server.</p> <p>For more information about sticky sessions, see Sticky Session.</p>

Parameter	Description
Sticky Session Type	<p>Specifies the type of sticky sessions. After the sticky session is enabled, you need to select a sticky session type:</p> <ul style="list-style-type: none">• Source IP address: The source IP address of each request is calculated using the consistent hashing algorithm to obtain a unique hashing key, and all backend servers are numbered. The system allocates the client to a particular server based on the generated key. This enables requests from different clients to be routed and ensures that a client is directed to the same server that it was using previously.• Load balancer cookie: The load balancer generates a cookie after receiving a request from the client. All subsequent requests with the cookie are routed to the same backend server.• Application cookie: The application deployed on the backend server generates a cookie after receiving the first request from the client. All subsequent requests with the cookie are routed to the same backend server. <p>NOTE</p> <ul style="list-style-type: none">• Source IP address is available when you have selected TCP or UDP for Backend Protocol.• Load balancer cookie and Application cookie are available when you have selected HTTP or HTTPS for Backend Protocol.
Stickiness Duration (min)	<p>Specifies the time that sticky sessions are maintained, in minutes.</p> <ul style="list-style-type: none">• Sticky sessions at Layer 4: 1 to 60• Sticky sessions at Layer 7: 1 to 1440
Description	<p>Provides supplementary information about the backend server group.</p>

4. Click **Next** to add backend servers and configure health check based on [Table 2-22](#). For more information about health checks, see [Health Check](#).

Table 2-22 Parameters required for configuring a health check

Parameter	Description
Health Check	<p>Specifies whether to enable health checks.</p> <p>If the health check is enabled, click  next to Advanced Settings to set health check parameters.</p>

Parameter	Description
Health Check Protocol	<ul style="list-style-type: none">• The health check protocol can be TCP or HTTP.• If the protocol of the backend server group is UDP, the health check protocol is UDP by default.
Domain Name	<p>Specifies the domain name that will be used for health checks. This parameter is mandatory if the health check protocol is HTTP. By default, the private IP address of each backend server is used.</p> <p>You can also specify a domain name that consists of at least two labels separated by periods (.). Use only letters, digits, and hyphens (-). Do not start or end strings with a hyphen. Max total: 100 characters. Max label: 63 characters.</p>
Health Check Port	<p>Specifies the port that will be used by the load balancer to check the health of backend servers. The port number ranges from 1 to 65535.</p> <p>NOTE By default, the service port on each backend server is used. You can also specify a port for health checks.</p>
Path	<p>Specifies the health check URL, which is the destination on backend servers for health checks. This parameter is mandatory if the health check protocol is HTTP. The path can contain 1 to 80 characters and must start with a slash (/).</p> <p>The path can contain letters, digits, hyphens (-), slashes (/), periods (.), question marks (?), number signs (#), percent signs (%), ampersands (&).</p>
Interval (s)	<p>Specifies the maximum time between two consecutive health checks, in seconds.</p> <p>The interval ranges from 1 to 50.</p>
Timeout (s)	<p>Specifies the maximum time required for waiting for a response from the health check, in seconds. The value ranges from 1 to 50.</p>
Healthy Threshold	<p>Specifies the number of consecutive successful health checks required for declaring a backend server healthy. The value ranges from 1 to 10.</p>
Unhealthy Threshold	<p>Specifies the number of consecutive failed health checks required for declaring a backend server unhealthy. The value ranges from 1 to 10.</p>

5. Click **Next**.
6. Confirm the specifications and click **Create Now**.

2.4.3 Controlling Traffic Distribution

2.4.3.1 Load Balancing Algorithms

Overview

Load balancers receive requests from clients and forward them to backend servers in one or more AZs. Each load balancer has at least a listener and a backend server. The load balancing algorithm you select when you create the backend server group determines how requests are distributed.

Shared load balancers support the following load balancing algorithms: weighted round robin, weighted least connections, and source IP hash.

You can select the load balancing algorithm that best suits your needs.

Table 2-23 Load balancing algorithms

Load Balancing Algorithm	Description
Weighted round robin	Routes requests to backend servers in sequence based on their weights.
Weighted least connections	Routes requests to backend servers with the smallest connections-to-weight ratio.
Consistent hashing: Source IP hash	Consistent hashing: Calculates the request fields using the consistent hashing algorithm to obtain a hash value and routes requests with the same hash value to the same backend server, even if the number of backend servers in the backend server group changes. Source IP hash: Calculates the source IP address of each request and routes requests from the same source IP address to the same backend server.

How Load Balancing Algorithms Work

Shared load balancers support weighted round robin, weighted least connections, and source IP hash algorithms.

Weighted Round Robin

Figure 2-9 shows an example of how requests are distributed using the weighted round robin algorithm. Two backend servers are in the same AZ and have the same weight, and each server receives the same proportion of requests.

Figure 2-9 Traffic distribution using the weighted round robin algorithm

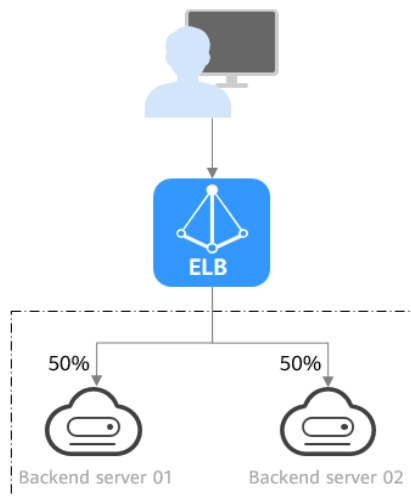


Table 2-24 Weighted round robin

Description	Requests are routed to backend servers in sequence based on their weights. Backend servers with higher weights receive proportionately more requests, whereas equal-weighted servers receive the same number of requests.
When to Use	<p>This algorithm is typically used for short connections, such as HTTP connections.</p> <ul style="list-style-type: none"> • Flexible load balancing: When you need more refined load balancing, you can set a weight for each backend server to specify the percentage of requests to each server. For example, you can set higher weights to backend servers with better performance so that they can process more requests. • Dynamic load balancing: You can adjust the weight of each backend server in real time when the server performance or load fluctuates.
Disadvantages	<ul style="list-style-type: none"> • You need to set a weight for each backend server. If you have a large number of backend servers or your services require frequent adjustments, setting weights would be time-consuming. • If the weights are inappropriate, the requests processed by each server may be imbalanced. As a result, you may need to frequently adjust server weights.

Weighted Least Connections

Figure 2-10 shows an example of how requests are distributed using the weighted least connections algorithm. Two backend servers are in the same AZ and have the same weight, 100 connections have been established with backend server 01,

and 50 connections have been established with backend server 02. New requests are preferentially routed to backend server 02.

Figure 2-10 Traffic distribution using the weighted least connections algorithm

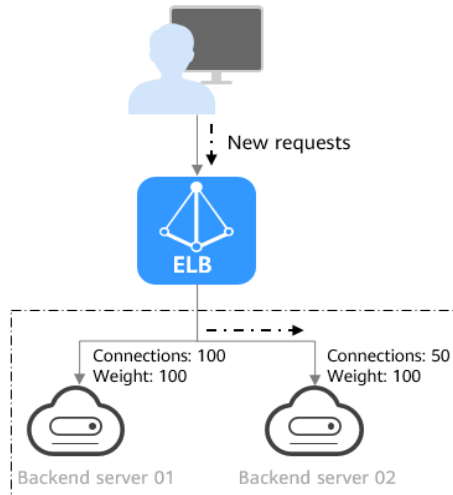


Table 2-25 Weighted least connections

Description	In addition to the number of active connections established with each backend server, each server is assigned a weight based on their processing capability. Requests are routed to the server with the lowest connections-to-weight ratio.
When to Use	<p>This algorithm is often used for persistent connections, such as connections to a database.</p> <ul style="list-style-type: none"> • Flexible load balancing: Load balancers distribute requests based on the number of established connections and the weight of each backend server and route requests to the server with the lowest connections-to-weight ratio. This helps prevent servers from being underloaded or overloaded. • Dynamic load balancing: When the number of connections to and loads on backend servers change, you can use the weighted least connection algorithm to dynamically adjust the requests distributed to each server in real time. • Stable load balancing: You can use this algorithm to reduce the peak loads on each backend server and improve service stability and reliability.

Disadvantages	<ul style="list-style-type: none"> • Complex calculation: The weighted least connections algorithm needs to calculate and compare the number of connections established with each backend server in real time before selecting a server to route requests. • Dependency on connections to backend servers: The algorithm routes requests based on the number of connections established with each backend server. If monitoring data is inaccurate or outdated, requests may not be distributed evenly across backend servers. The algorithm can only collect statistics on the connections between a given load balancer and a backend server, but cannot obtain the total number of connections to the backend server if it is associated with multiple load balancers. • Too many loads on new servers: If existing backend servers have to handle a large number of requests, new requests will be routed to new backend servers. This may deteriorate new servers or even cause them to fail.
----------------------	--

Source IP Hash

Figure 2-11 shows an example of how requests are distributed using the source IP hash algorithm. Two backend servers are in the same AZ and have the same weight. If backend server 01 has processed a request from IP address A, the load balancer will route new requests from IP address A to backend server 01.

Figure 2-11 Traffic distribution using the source IP hash algorithm

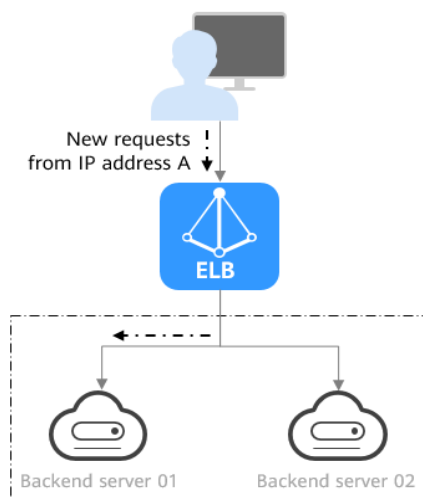


Table 2-26 Source IP hash

Description	The source IP hash algorithm calculates the source IP address of each request and routes requests from the same IP address to the same backend server.
--------------------	--

When to Use	<p>This algorithm is often used for applications that need to maintain user sessions or state.</p> <ul style="list-style-type: none">• Session persistence: Source IP hash ensures that requests with the same source IP address are distributed to the same backend server.• Data consistency: Requests with the same hash value are distributed to the same backend server.• Load balancing: In scenarios that have high requirements for load balancing, this algorithm can distribute requests to balance loads among servers.
Disadvantages	<ul style="list-style-type: none">• Imbalanced loads across servers: This algorithm tries its best to ensure request consistency when backend servers are added or removed. If the number of backend servers decreases, some requests may be redistributed, causing imbalanced loads across servers.• Complex calculation: This algorithm calculates the hash values of requests based on hash factors. If servers are added or removed, some requests may be redistributed, making calculation more difficult.

Changing a Load Balancing Algorithm

1. Go to the [backend server group list page](#).
2. On the **Backend Server Groups** page, locate the target backend server group and click **Edit** in the **Operation** column.
3. In the **Modify Backend Server Group** dialog box, change the load balancing algorithm.
4. Click **OK**.

NOTE

The change is applied immediately and will be used to route requests over new connections. However, the previous load balancing algorithm will still be used to route requests over established connections.

2.4.3.2 Sticky Session

Sticky sessions ensure that requests from a client always get routed to the same backend server before a session elapses.

Here is an example that describes how sticky session works. Assume that you have logged in to a server. After a while, you send another request. If sticky sessions are not enabled, the request may be routed to another server, and you will be asked to log in again. If sticky sessions are enabled, all your requests are processed by the same server, and you do not need to repeatedly log in.

Differences Between Sticky Sessions at Layer 4 and Layer 7

The following table describes the differences of sticky sessions at Layer 4 at Layer 7.

Table 2-27 Sticky session comparison

OSI Layer	Listener Protocol	Sticky Session Type	Stickiness Duration	Scenarios Where Sticky Sessions Become Invalid
Layer 4	TCP or UDP	<p>Source IP address: The source IP address of each request is calculated using the consistent hashing algorithm to obtain a unique hashing key, and all backend servers are numbered. The system allocates the client to a particular server based on the generated key. This allows requests from the same IP address are forwarded to the same backend server.</p>	<ul style="list-style-type: none"> • Default: 20 minutes • Maximum: 60 minutes • Range: 1 minute to 60 minutes 	<ul style="list-style-type: none"> • Source IP addresses of the clients change. • The session stickiness duration has been reached.

OSI Layer	Listener Protocol	Sticky Session Type	Stickiness Duration	Scenarios Where Sticky Sessions Become Invalid
Layer 7	HTTP or HTTPS	<ul style="list-style-type: none"> • Load balancer cookie: The load balancer generates a cookie after receiving a request from the client. All subsequent requests with the cookie are routed to the same backend server. • Application cookie: The application deployed on the backend server generates a cookie after receiving the first request from the client. All subsequent requests with the cookie are routed to the same backend server. 	<ul style="list-style-type: none"> • Default: 20 minutes • Maximum: 1,440 minutes • Range: 1 minute to 1,440 minutes 	<ul style="list-style-type: none"> • If requests sent by the clients do not contain a cookie, sticky sessions will not take effect. • Requests from the clients exceed the session stickiness duration.

 NOTE

- If you set **Load Balancing Algorithm** to **Source IP hash**, you do not need to manually enable and configure **Sticky Session**. Source IP hash allows requests from the same client to be directed to the same server.
- If you set **Load Balancing Algorithm** to **Weighted round robin** or **Weighted least connections**, you need to manually enable and configure **Sticky Session**.

Notes and Constraints

- If you use **Cloud Connect connection**, **Direct Connect** or **VPN** to access ELB, you must select **Source IP hash** as the load balancing algorithm and disable sticky sessions for ELB.

- Shared load balancers support three types of sticky session: **Source IP address**, **Load balancer cookie**, and **Application cookie**.

 **NOTE**

- For HTTP and HTTPS listeners, enabling or disabling sticky sessions may cause few seconds of service interruption.
- If you enable sticky sessions, traffic to backend servers may be unbalanced. If this happens, disable sticky sessions and check the requests received by each backend server.

Enabling or Disabling Sticky Session

1. Go to the [backend server group list page](#).
2. On the **Backend Server Groups** page, locate the backend server group and click **Edit** in the **Operation** column.
3. In the **Modify Backend Server Group** dialog box, enable or disable **Sticky Session**.
If you enable it, select the sticky session type, and set the session stickiness duration.
4. Click **OK**.

2.4.4 Changing a Backend Server Group

Scenario

This section describes how you can change the default backend server group configured for a listener.

TCP or UDP listeners forward requests to the default backend server groups.

HTTP or HTTPS listeners forward requests based on the priorities of the forwarding policies. If you do not add a forwarding policy, the listener will route the requests to the default backend server group.

Notes and Constraints

- The backend server group cannot be changed if redirection is enabled.
- The backend protocol of the backend server group must match the frontend protocol of the listener. For details, see [Table 2-19](#).
- You can only associate a backend server group that is not used by any listener with a shared load balancer.

Procedure

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the target load balancer and click its name.
3. On the **Listeners** tab, locate the target listener and click its name.
4. On the **Summary** tab, click **Change Backend Server Group** on the right of **Default Backend Server Group** area.
5. In the displayed dialog box, click the server group name box.
Select a backend server group from the drop-down list or create a group.

- a. Click the name of the backend server group or enter the name in the search box to search for the target group.
- b. Click **Create Backend Server Group**. After the backend server group is created, click the refresh icon.

 **NOTE**

The backend protocol of the new backend server group must match the frontend protocol of the listener.

6. Click **OK**.

2.4.5 Managing a Backend Server Group

You can manage a backend server group as required.

Enabling Modification Protection

You can enable the modification protection for a backend server group to prevent the backend servers in it from being modified or deleted by accident.

Enabling the modification protection option for a backend server group will prohibit any change to both the group and its backend servers.

1. Go to the [backend server group list page](#).
2. On the **Backend Server Groups** page, locate the backend server group and click its name.
3. On the **Summary** tab, click **Configure** next to **Modification Protection**.
4. In the **Configure Modification Protection** dialog box, enable **Modification Protection**.
5. Click **OK**.

 **NOTE**

Disable **Modification Protection** if you want to delete a backend server group or modify its settings.

Viewing a Backend Server Group

You can view the details of a backend server group.

1. Go to the [backend server group list page](#).
2. On the **Backend Server Groups** page, click the name of the backend server group.
3. Click different tabs to view the required information.
 - a. On the **Summary** tab, view the basic information (name, ID, backend protocol) and health check settings.
 - b. On the **Backend Servers** tab, view the servers that have been added to the backend server group.

Deleting a Backend Server Group

Before deleting a backend server group, you need to:

- Disassociate it from the listener. For details, see [Changing a Backend Server Group](#).
 - Ensure the backend server group is not used by a forwarding policy of an HTTP or HTTPS listener.
1. Go to the [backend server group list page](#).
 2. On the **Backend Server Groups** page, locate the backend server group and click **Delete** in the **Operation** column.
 3. In the displayed dialog box, click **OK**.

2.5 Backend Server

2.5.1 Backend Server Overview

Backend servers receive and process requests from the associated load balancer.

If the incoming traffic increases, you can add more backend servers to ensure the stability and reliability of applications and eliminating SPOFs. If the incoming traffic decreases, you can remove some backend servers to reduce the cost.

If the load balancer is associated with an AS group, instances are automatically added to or removed from the load balancer.

You can only add servers in the same VPC as the load balancer. For details, see [Cloud Servers](#).

Precautions

- It is recommended that you select backend servers running the same OS for easier management and maintenance.
- The load balancer checks the health of each server added to the associated backend server group if you have configured health check for the backend server group. If the backend server responds normally, the load balancer will consider it healthy. If the backend server does not respond normally, the load balancer will periodically check its health until the backend server is considered healthy.
- If a backend server is stopped or restarted, connections established with the server will be disconnected, and data being transmitted over these connections will be lost. To avoid this from happening, configure the retry function on the clients to prevent data loss.
- If you enable sticky sessions, traffic to backend servers may be unbalanced. If this happens, disable sticky sessions and check the requests received by each backend server.

Notes and Constraints

- A maximum of 500 backend servers can be added to a backend server group.
- Inbound security group rules must be configured to allow traffic over the port of each backend server and health check port. For details, see [Security Group and Network ACL Rules](#).

Backend Server Weights

You need to set a weight for each backend server in a backend server group to receive requests. The higher the weight you have configured for a backend server, the more requests the backend server receives.

The weight ranges from **0** to **100**. If you set the weight of a cloud server to **0**, new requests will not be routed to this server.

Three load balancing algorithms allow you to set weights to backend servers, as described in [Table 2-28](#). For more information about load balancing algorithms, see [Load Balancing Algorithms](#).

Table 2-28 Server weights in different load balancing algorithms

Load Balancing Algorithm	Weight Setting
Weighted round robin	<ul style="list-style-type: none">• If none of the backend servers have a weight of 0, the load balancer routes requests to backend servers based on their weights. Backend servers with higher weights receive proportionately more requests.• If two backend servers have the same weights, they receive the same number of requests.
Weighted least connections	<ul style="list-style-type: none">• If none of the backend servers have a weight of 0, the load balancer calculates the load of each backend server using the formula (Overhead = Number of current connections/Backend server weight).• The load balancer routes requests to the backend server with the lowest overhead.
Source IP hash	<ul style="list-style-type: none">• If none of the backend servers have a weight of 0, requests from the same client are routed to the same backend server within a period of time.• If the weight of a backend server is 0, no requests are routed to this backend server.

2.5.2 Security Group and Network ACL Rules

To ensure normal communications between the load balancer and backend servers, you need to check the security group and network ACL rules.

When backend servers receive requests from the load balancer, source IP addresses are translated into those in 100.125.0.0/16.

- Security group rules of backend servers must allow traffic from the 100.125.0.0/16 to backend servers. For details about how to configure security group rules, see [Configuring Security Group Rules](#).
- Network ACL rules are optional for subnets. If network ACL rules are configured for the subnet where the backend servers are deployed, the rules must allow traffic from the backend subnet of the load balancer to the subnet

of the backend servers. For details about how to configure network ACL rules, see [Configuring Network ACL Rules](#).

NOTE

If **Transfer Client IP Address** is enabled for the TCP or UDP listeners, network ACL and security group rules will not take effect. You can use access control to limit which IP addresses are allowed to access the listener. Learn how to configure [What Is Access Control?](#)

Notes and Constraints

- If health check is enabled for a backend server group, security group rules must allow traffic from the health check port over the health check protocol.
- If UDP is used for health check, there must be a rule that allows ICMP traffic. If there is no such rule, the health of the backend servers cannot be checked.

Configuring Security Group Rules

If you have no VPCs when creating a server, the system automatically creates one for you. Default security group rules allow only communications among the servers in the VPC. To ensure that the load balancer can communicate with these servers over both the frontend port and health check port, configure inbound rules for security groups containing these servers.


1. Log in to the management console.
2. In the upper left corner of the page, click  and select the desired region and project.
3. Under **Compute**, click **Elastic Cloud Server**.
4. On the **Elastic Cloud Server** page, click the name of the ECS that has been added to a backend server group.
The page providing details about the ECS is displayed.
5. Click **Security Groups**, locate the security group, and view security group rules.
6. Click the ID of a security group rule or **Modify Security Group Rule**. The security group details page is displayed.
7. On the **Inbound Rules** tab, click **Add Rule**. Configure an inbound rule based on [Table 2-29](#).

Table 2-29 Security group rules

Backend Protocol	Policy	Protocol & Port	Source IP Address
HTTP	Allow	Protocol: TCP Port: the port used by the backend server and health check port	100.125.0.0/16

Backend Protocol	Policy	Protocol & Port	Source IP Address
TCP	Allow	Protocol: TCP Port: health check port	100.125.0.0/16
UDP	Allow	Protocol: UDP and ICMP Port: health check port	100.125.0.0/16

8. Click **OK**.

Configuring Network ACL Rules



To control traffic in and out of a subnet, you can associate a network ACL with the subnet. Network ACL rules control access to subnets and add an additional layer of defense to your subnets. Default network ACL rules reject all inbound and outbound traffic. If the subnet of a load balancer or associated backend servers has a network ACL associated, the load balancer cannot receive traffic from the Internet or route traffic to backend servers, and backend servers cannot receive traffic from and respond to the load balancer.

Configure an inbound network ACL rule to allow access from 100.125.0.0/16.

ELB translates the public IP addresses used to access backend servers into private IP addresses in 100.125.0.0/16. You cannot configure network ACL rules to prevent public IP addresses from accessing backend servers.

NOTE

Network ACL rules configured for the backend subnet of the load balancer will not restrict the traffic from the clients to the load balancer. If these rules are configured, the clients can directly access the load balancer. To control access to the load balancer, configure access control for all listeners added to the load balancer. For details, see [What Is Access Control?](#)

1. Log in to the management console.
2. In the upper left corner of the page, click  and select the desired region and project.
3. Click  in the upper left corner to display **Service List** and choose **Networking > Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control > Network ACLs**.
5. In the network ACL list, locate the target network ACL and click its name.
6. On the **Inbound Rules** or **Outbound Rules** tab, click **Add Rule** to add an inbound or outbound rule.
 - **Action:** Select **Allow**.
 - **Protocol:** The protocol must be the same as the backend protocol.
 - **Source:** Set it to **100.125.0.0/16**.

- **Source Port Range:** Select a port range.
 - **Destination:** Enter a destination address allowed in this direction. The default value is **0.0.0.0/0**, which indicates that traffic from all IP addresses is permitted.
 - **Destination Port Range:** Select a port range.
 - (Optional) **Description:** Describe the network ACL rule if necessary.
7. Click **OK**.

2.5.3 Cloud Servers

When you use ELB to route requests, ensure that at least one backend server is running properly and can receive requests routed by the load balancer.

After a backend server is unbound from a load balancer, the backend server does not receive requests forwarded by the load balancer, but the backend server is disassociated from the load balancer. You can add the backend server to the backend server group again when traffic increases or the reliability needs to be enhanced.

Notes and Constraints

- Only servers in the same VPC as the load balancer can be added.
- ECSs and BMSs can be added as backend servers. If **Transfer Client IP Address** is enabled for the listeners of a shared load balancer, only BMSs with **certain flavors** can be added as backend servers.

Adding a Cloud Server

1. Go to the [backend server group list page](#).
2. On the **Backend Server Groups** page, click the name of the backend server group.
3. Switch to the **Backend Servers** tab and click **Add** on the right of the **Cloud Servers** area.
4. Search for backend servers using specified keywords.
5. Specify the weights and ports for the backend servers, and click **Finish**.
Backend server ports can be set in batches.

Modifying Cloud Server Ports/Weights

1. Go to the [backend server group list page](#).
2. On the **Backend Server Groups** page, click the name of the target backend server group.
3. On the **Backend Servers** tab, click **Cloud Servers**.
4. Select the cloud servers and click **Modify Weight** up above the cloud server list.
5. In the displayed dialog box, modify the weights as you need.
 - Changing the weight of a single cloud server: Set the weight in the **Weight** column.
 - Modifying the weights of multiple cloud servers: Select the target cloud servers and set the weight next to **Batch Modify Weights** and click **OK**.

 NOTE

You can set the weights of multiple cloud servers to **0** to block them from receiving requests routed by each load balancer.

6. Click **OK**.

Removing a Cloud Server

 NOTE

If a cloud server is removed, requests are still routed to it. This is because a persistent connection is established between the load balancer and the backend server and requests are routed to this server until the TCP connection times out. If no data is transmitted over this TCP connection after it times out, ELB disconnects the connection.

1. Go to the [backend server group list page](#).
2. On the **Backend Server Groups** page, click the name of the target backend server group.
3. Switch to the **Backend Servers** tab and click **Cloud Servers**.
4. Select the cloud servers you want to remove and click **Remove** above the cloud server list.
5. In the displayed dialog box, click **OK**.

2.6 Health Check

2.6.1 Health Check

ELB periodically sends requests to backend servers to check whether they can process requests. This process is called health check.

If a backend server is detected unhealthy, the load balancer will stop routing requests to it. After the backend server recovers, the load balancer will resume routing requests to it.

If backend servers have to handle large number of requests, frequent health checks may overload the backend servers and cause them to respond slowly. To address this problem, you can prolong the health check interval or use TCP or UDP instead of HTTP. You can also disable health check. If you choose to disable health check, requests may be routed to unhealthy servers, and service interruptions may occur.

Health Check Protocol

You can configure health checks when configuring backend server groups. Generally, you can use the default setting or select a different health check protocol as you need.

If you want to modify health check settings, see details in [Enabling or Disabling Health Check](#).

Select a health check protocol that matches the backend protocol as described in [Table 2-30](#).

Table 2-30 The backend protocol and health check protocols (shared load balancers)

Backend Protocol	Health Check Protocol
TCP	TCP or HTTP
UDP	UDP
HTTP	TCP or HTTP
HTTPS	TCP or HTTP

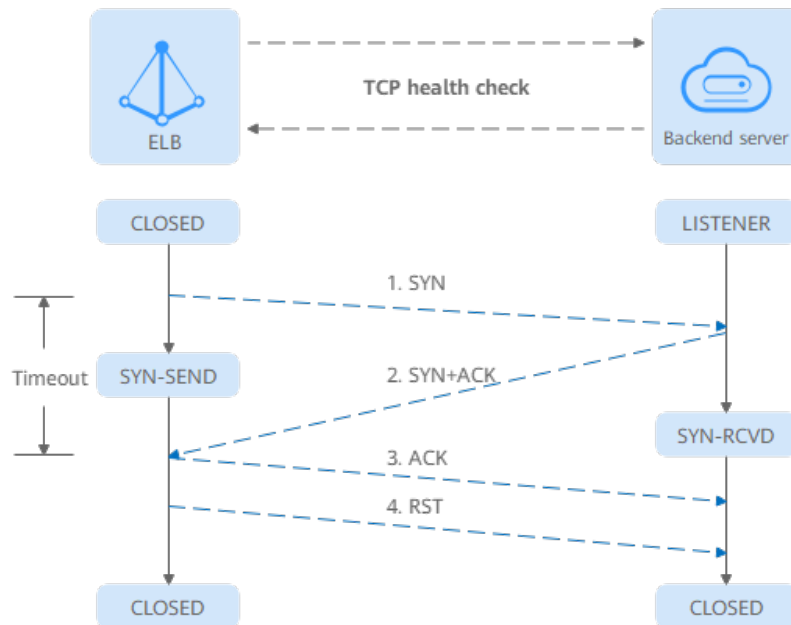
Health Check Source IP Address

A shared load balancer uses an IP address in 100.125.0.0/16 to send requests to backend servers and verify their health status. To perform health checks, ensure that the security group rules of the backend server allow access from 100.125.0.0/16. For details, see [Security Group and Network ACL Rules](#).

TCP Health Check

For TCP, HTTP, and HTTPS backend protocols, you can use TCP to initiate three-way handshakes to obtain the statuses of backend servers.

Figure 2-12 TCP health check



The TCP health check process is as follows:

1. The load balancer sends a TCP SYN packet to the backend server (in the format of $\{Private\ IP\ address\}:\{Health\ check\ port\}$).
2. The backend server returns an SYN-ACK packet.

- If the load balancer does not receive the SYN-ACK packet within the timeout duration, it declares that the backend server is unhealthy and sends an RST packet to the backend server to terminate the TCP connection.
- If the load balancer receives the SYN-ACK packet from the backend server within the timeout duration, it sends an ACK packet to the backend server and declares that the backend server is healthy. After that, the load balancer sends an RST packet to the backend server to terminate the TCP connection.

NOTICE

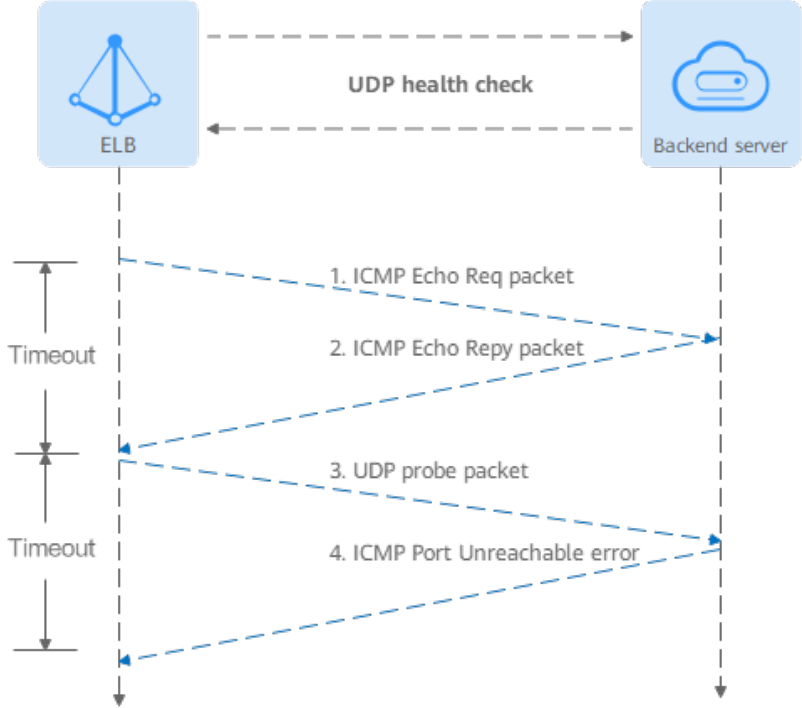
After a successful TCP three-way handshake, an RST packet will be sent to close the TCP connection. The application on the backend server may consider this packet a connection error and reply with a message, for example, "Connection reset by peer". To avoid this issue, take either of the following actions:

- Use [HTTP Health Check](#).
- Have the backend server ignore the connection error.

UDP Health Check

For UDP backend protocol, ELB sends ICMP and UDP probe packets to backend servers to check their health.

Figure 2-13 UDP health check



The UDP health check process is as follows:

1. The load balancer sends an ICMP Echo Request packet to the backend server.
 - If the load balancer does not receive an ICMP Echo Reply packet within the health check timeout duration, the backend server is declared unhealthy.
 - If the load balancer receives an ICMP Echo Reply packet within the timeout period, it sends a UDP probe packet to the backend server.
2. If the load balancer does not receive an ICMP Port Unreachable error within the health check timeout duration, it declares the backend server is healthy. If the load balancer receives an ICMP Port Unreachable error, the backend server is declared unhealthy.

NOTE

- If there is a large number of concurrent requests, the health check result may be different from the actual health of the backend server.
If the backend server runs Linux, it may limit the rate of ICMP packets as a defense against ping flood attacks. In this case, even if there is a service exception, ELB will not receive the error message "port XX unreachable", and the server will still be determined healthy. This causes the health check result to be different from the actual health of the backend server.
- The UDP probe packet's payload has no significance and is simply used to fill the packet with data. Typically, the payload is set to "H". Clients should not attempt to interpret its content.

HTTP Health Check

You can also configure HTTP health checks to obtain server statuses through HTTP GET requests if you select TCP, HTTP, or HTTPS as the backend protocol. [Figure 2-14](#) shows how an HTTP health check works.

Figure 2-14 HTTP health check



The HTTPS health check process is as follows:

1. The load balancer sends an HTTP GET request to the backend server (in format of *{Private IP address}:{Health check port}{Health check path}*). (You can specify a domain name when configuring a health check.)
2. The backend server returns an HTTP status code to ELB.
 - If the load balancer receives the status code within the health check timeout duration, it compares the status code with the preset one. If the status codes are the same, the backend server is declared healthy.
 - If the load balancer does not receive any response from the backend server within the health check timeout duration, it declares the backend server is unhealthy.

 NOTE

In an HTTP health check, the User-Agent header identifies that the requests are sent for health checks. The value of User-Agent may be adjusted based on service requirements. So it is not recommended to rely on this header for verification or judgment.

Health Check Time Window

Health checks greatly improve service availability. However, if health checks are too frequent, service availability will be compromised. To avoid the impact, ELB declares a backend server healthy or unhealthy after several consecutive health checks.

The health check time window is determined by the factors in [Table 2-31](#).

Table 2-31 Factors affecting the health check time window

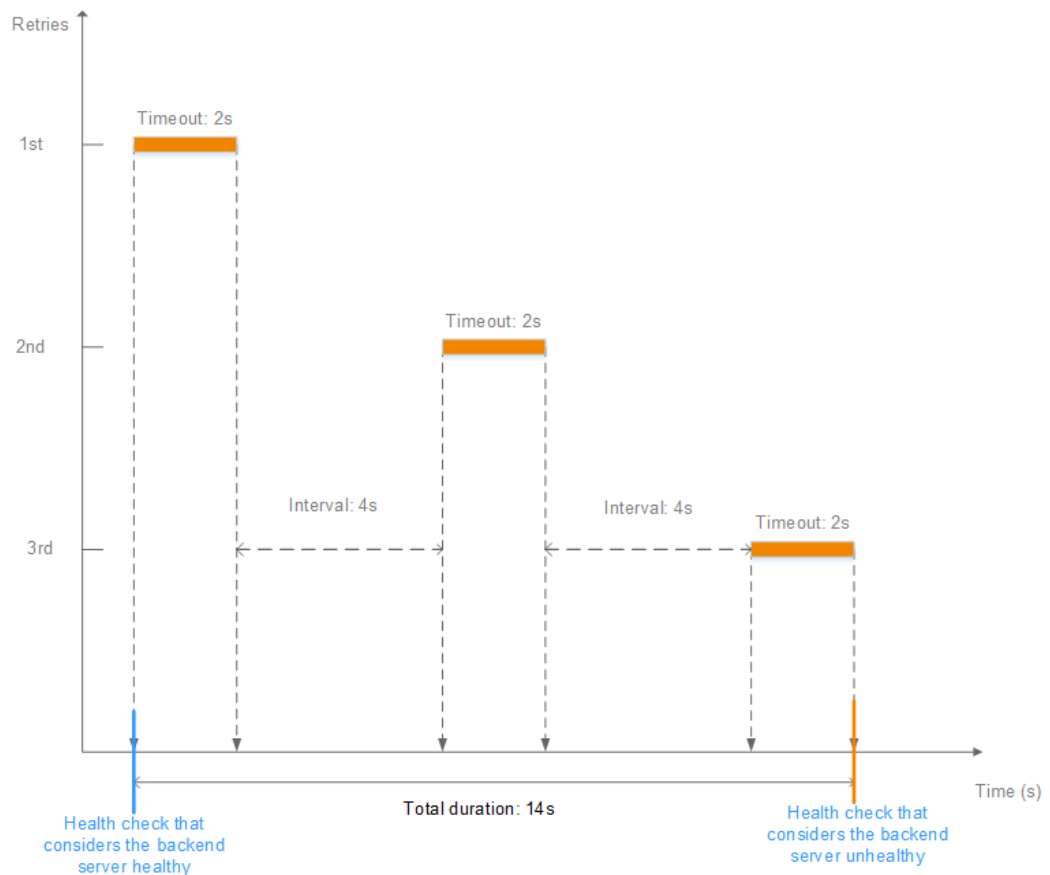
Factor	Description
Check Interval	How often health checks are performed.
Timeout Duration	How long the load balancer waits for the response from the backend server.
Health Check Threshold	The number of consecutive successful or failed health checks required for determining whether the backend server is healthy or unhealthy.

The following is a formula for you to calculate the health check time window:

- Time window for a backend server to be detected healthy = Timeout duration x Healthy threshold + Interval x (Healthy threshold - 1)
- Time window for a backend server to be detected unhealthy = Timeout duration x Unhealthy threshold + Interval x (Unhealthy threshold - 1)

As shown in [Figure 2-15](#), if the health check interval is 4s, the health check timeout duration is 2s, and unhealthy threshold is 3, the time window for a backend server to be considered unhealthy is calculated as follows: $2 \times 3 + 4 \times (3 - 1) = 14s$.

Figure 2-15 Health check timeout duration



Rectifying an Unhealthy Backend Server

If a backend server is detected unhealthy, see [How Do I Troubleshoot an Unhealthy Backend Server?](#)

2.6.2 Enabling or Disabling Health Check

Scenarios

This section describes how you can enable or disable the health check option.

After the protocol is changed, the load balancer uses the new protocol to check the health of backend servers. The load balancer continues to route traffic to the backend servers after they are detected healthy.

Before the new configurations take effect, the load balancer may return the HTTP 503 error code to the clients.

Notes and Constraints

- The health check protocol can be different from the backend protocol.
- To reduce the vCPU usage of the backend servers, it is recommended that you use TCP for health checks. If you want to use HTTP for health checks, you can use static files to return the health check results.

- If health check is enabled, security group rules must allow traffic from the health check port to the backend servers over the health check protocol. For details, see [Security Group and Network ACL Rules](#).

NOTE

After you enable health check, the load balancer immediately checks the health of backend servers.

- If a backend server is detected healthy, the load balancer will start routing requests to it over new connections based on the configured loading balancing algorithms and weights.
- If a backend server is detected unhealthy, the load balancer will stop routing traffic to it.

Enabling Health Check

1. Go to the [backend server group list page](#).
2. On the **Backend Server Groups** page, locate the backend server group and click its name.
3. On the **Summary** page, click **Health Check** on the right.
4. In the **Configure Health Check** dialog box, configure the parameters based on [Table 2-32](#).

Table 2-32 Parameters required for configuring health check

Parameter	Description
Health Check	Specifies whether to enable health checks. NOTE When the health check is enabled or disabled, the number of healthy or unhealthy backend servers may temporarily fluctuate but will stabilize after a monitoring period.
Health Check Protocol	Specifies the protocol that will be used by the load balancer to check the health of backend servers. If the protocol of the backend server group is UDP, the health check protocol is UDP by default. Shared load balancers support TCP and HTTP.
Domain Name	Specifies the domain name that will be used for health checks. This parameter is mandatory if the health check protocol is HTTP. <ul style="list-style-type: none">• You can use the private IP address of the backend server as the domain name.• You can also specify a domain name that consists of at least two labels separated by periods (.). Use only letters, digits, and hyphens (-). Do not start or end strings with a hyphen. Max total: 100 characters. Max label: 63 characters.

Parameter	Description
Health Check Port	Specifies the port that will be used by the load balancer to check the health of backend servers. The port number ranges from 1 to 65535 . NOTE By default, the service port on each backend server is used. You can also specify a port for health checks.
Path	Specifies the health check URL, which is the destination on backend servers for health checks. This parameter is mandatory if the health check protocol is HTTP. The path can contain 1 to 80 characters and must start with a slash (/). If the backend server group is associated with a shared load balancer, the path can contain letters, digits, hyphens (-), slashes (/), periods (.), question marks (?), percent signs (%), ampersands (&), and underscores (_).
Interval (s)	Specifies the maximum time between two consecutive health checks, in seconds. The interval ranges from 1 to 50 .
Timeout (s)	Specifies the maximum time required for waiting for a response from the health check, in seconds. The value ranges from 1 to 50 .
Healthy Threshold	Specifies the number of consecutive successful health checks required for declaring a backend server healthy. The value ranges from 1 to 10 .
Unhealthy Threshold	Specifies the number of consecutive failed health checks required for declaring a backend server unhealthy. The value ranges from 1 to 10 .

5. Click **OK**.

Disabling Health Check

1. Go to the [backend server group list page](#).
2. On the **Backend Server Groups** page, click the name of the target backend server group.
3. On the **Summary** page, click **Health Check** on the right.
4. In the **Configure Health Check** dialog box, disable health check.
5. Click **OK**.

2.7 Security

2.7.1 Transfer Client IP Address

Scenarios

Generally, shared load balancers use IP addresses in 100.125.0.0/16 to communicate with backend servers. If you want a load balancer to communicate with backend servers using real IP addresses of the clients, you can enable **Transfer Client IP Address** to pass the IP addresses of the clients to backend servers.

[Table 2-33](#) lists whether you can enable or disable this feature.

Table 2-33 Transfer client IP address support

Listener Type	Enabling Transfer Client IP Address	Disabling Transfer Client IP Address
TCP and UDP	Supported	Supported
HTTP and HTTPS	Enabled by default	Not supported

Notes and Constraints

- When you enable or disable **Transfer Client IP Address**, if the listener has backend servers associated, traffic to this listener will be interrupted for about 10 seconds. The interruption duration is twice the health check interval configured for the backend server group.
- If **Transfer Client IP Address** is enabled, a server cannot serve as both a backend server and a client. This is because backend server will think the packet from the client is sent by itself and will not return a response packet to the load balancer. As a result, the return traffic will be interrupted.
- If a backend server has been associated with the listener and health checks are enabled, enabling this function will check the health of the backend server, and traffic to this server will be interrupted for one or two health check intervals.
- If **Transfer Client IP Address** is enabled, traffic, such as unidirectional download or push traffic, may be interrupted when backend servers are being migrated. After backend servers are migrated, retransmit the packets to restore the traffic.

Enabling Transfer Client IP Address

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
3. You can use either of the following methods to enable the feature:
 - On the **Listeners** tab, locate the listener and click **Edit** in the **Operation** column.
 - Click the name of the target listener. On the **Summary** tab, click **Edit** on the top right corner.

4. In the displayed dialog box, enable **Transfer Client IP Address**.
5. Confirm the configurations and click **OK**.

 **NOTE**

After **Transfer Client IP Address** is enabled, configure security groups, network ACLs, and OS and software security policies so that IP addresses of the clients can access these backend servers.

Disabling Transfer Client IP Address

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
3. You can use either of the following methods to disable the feature:
 - On the **Listeners** tab, locate the listener and click **Edit** in the **Operation** column.
 - Click the name of the target listener. On the **Summary** tab, click **Edit** on the top right corner.
4. In the displayed dialog box, disable **Transfer Client IP Address**.
5. Confirm the configurations and click **OK**.

Alternatives for Obtaining the IP Address of a Client

You can obtain the IP address of a client in the ways listed in [Table 2-34](#).

Table 2-34 Alternatives

Listener Type	Alternatives
TCP	Configuring the TOA Module
HTTP and HTTPS	Layer 7 Load Balancing

2.7.2 SNI Certificate

Server Name Indication (SNI) is an extension of the Transport Layer Security (TLS) protocol. It is used when a server uses multiple domain names and certificates.

Scenarios

If you have an application that can be accessed through multiple domain names and each domain name uses a different certificate, you can enable SNI when you add an HTTPS listener.

After SNI is enabled, you need to select SNI certificates based on the domain names. The client submits the requested domain name while sending an SSL handshake. Once receiving the request, the load balancer searches for the certificate based on the domain name. If the certificate is found, this certificate will be used for authentication. If no SNI certificates are found, the server certificate is used for authentication.

Notes and Constraints

- After SNI is enabled, select an SNI certificate by referring to [Adding a Certificate](#).
- SNI can be only enabled for HTTPS listeners.
- An HTTPS listener can have up to 30 SNI certificates. All the certificates can have up to 30 domain names.

Restrictions

- You must specify at least one domain name for each SNI certificate. The domain name must be the same as that in the certificate.
- A domain name can be used by both an ECC certificate and an RSA certificate. If there are two SNI certificates that use the same domain name, the ECC certificate is displayed preferentially.

How SNI Certificates and Domain Names Are Matched

- Domain names in an SNI certificate are matched as follows:
If the domain name of the certificate is *.test.com, a.test.com and b.test.com are supported, but a.b.test.com and c.d.test.com are not supported.
The domain name with the longest suffix is matched. If a certificate contains both *.b.test.com and *.test.com, a.b.test.com preferentially matches *.b.test.com.
- **cert-default** is the default certificate bound to the HTTPS listener, and **cert-test01** and **cert-test02** are SNI certificates.
The domain name of **cert-test01** is **www.test01.com** and that of **cert-test02** is **www.test02.com**.
If the domain name accessing the load balancer matches either of the domain names, the corresponding SNI certificate will be used for authentication. If no domain name is matched, the default server certificate is used for authentication.

Enabling SNI for an HTTPS Listener

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
3. Click **Listeners**, locate the listener, and click its name.
4. On the **Summary** tab, click **Configure** on the right of SNI.
5. Enable SNI and select an SNI certificate.
6. Click **OK**.

2.7.3 TLS Security Policy

Scenarios

HTTPS encryption is commonly used for applications that require secure transmission of data, such as banks and finance. When you add HTTPS listeners, you can select appropriate default security policies to improve security. A security

policy is a combination of TLS protocols of different versions and supported cipher suites.

You can only select the default security policies for HTTPS listeners added to a shared load balancer.

Adding a Default Security Policy

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
3. Under **Listeners**, click **Add Listener**.
4. On the **Add Listener** page, set **Frontend Protocol** to **HTTPS**.
5. Expand **Advanced Settings** and select a default security policy.

Table 2-35 lists the default security policies supported by shared load balancers.

Table 2-35 Default security policies

Name	TLS Versions	Cipher Suites
TLS-1-0	TLS 1.2 TLS 1.1 TLS 1.0	<ul style="list-style-type: none">• ECDHE-RSA-AES256-GCM-SHA384• ECDHE-RSA-AES128-GCM-SHA256• ECDHE-ECDSA-AES256-GCM-SHA384• ECDHE-ECDSA-AES128-GCM-SHA256
TLS-1-1	TLS 1.2 TLS 1.1	<ul style="list-style-type: none">• AES128-GCM-SHA256• AES256-GCM-SHA384
TLS-1-2	TLS 1.2	<ul style="list-style-type: none">• 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

Name	TLS Versions	Cipher Suites
TLS-1-2-Strict	TLS 1.2	<ul style="list-style-type: none"> • 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

 NOTE

- Shared load balancers support TLS 1.2 or earlier versions.
- The above table lists the cipher suites supported by ELB. Generally, clients also support multiple cipher suites. In actual use, the cipher suites supported by ELB and clients are used, and the cipher suites supported by ELB take precedence.

6. Confirm the configurations and go to the next step.

Differences Among Security Policies

Table 2-36 Differences Among Security Policies

Security Policy	tls-1-0	tls-1-1	tls-1-2	tls-1-0-inherit	tls-1-2-strict	tls-1-0-with-1-3	tls-1-2-fs-with-1-3	tls-1-2-fs	hybrid-policy-1-0
TLS version									
Protocol-TLS 1.3	N/A	N/A	N/A	N/A	N/A	Supported	Supported	Supported	N/A
Protocol-TLS 1.2	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Protocol-TLS 1.1	Supported	Supported	N/A	Supported	N/A	Supported	N/A	N/A	Supported

Security Policy	tls-1-0	tls-1-1	tls-1-2	tls-1-0-inherit	tls-1-2-strict	tls-1-0-with-1-3	tls-1-2-fs-with-1-3	tls-1-2-fs	hybrid-policy-1-0
Protocol-TLS 1.0	Supported	N/A	N/A	Supported	N/A	Supported	N/A	N/A	N/A
Cipher suite									
EDHE-RSA-AES128-GCM-SHA256	Supported	Supported	Supported	N/A	Supported	N/A	N/A	N/A	N/A
ECDHE-RSA-AES256-GCM-SHA384	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
ECDHE-RSA-AES128-SHA256	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
ECDHE-RSA-AES256-SHA384	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
AES128-GCM-SHA256	Supported	Supported	Supported	Supported	Supported	Supported	N/A	N/A	Supported
AES256-GCM-SHA384	Supported	Supported	Supported	Supported	Supported	Supported	N/A	N/A	Supported
AES128-SHA256	Supported	Supported	Supported	Supported	Supported	Supported	N/A	N/A	Supported
AES256-SHA256	Supported	Supported	Supported	Supported	Supported	Supported	N/A	N/A	Supported
ECDHE-RSA-AES128-SHA	Supported	Supported	Supported	Supported	N/A	Supported	N/A	N/A	Supported
ECDHE-RSA-AES256-SHA	Supported	Supported	Supported	Supported	N/A	Supported	N/A	N/A	Supported
AES128-SHA	Supported	Supported	Supported	Supported	N/A	Supported	N/A	N/A	Supported

Security Policy	tls-1-0	tls-1-1	tls-1-2	tls-1-0-inherit	tls-1-2-strict	tls-1-0-with-1-3	tls-1-2-fs-with-1-3	tls-1-2-fs	hybrid-policy-1-0
AES256-SHA	Supported	Supported	Supported	Supported	N/A	Supported	N/A	N/A	Supported
ECDHE-ECDSA-AES128-GCM-SHA256	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
ECDHE-ECDSA-AES128-SHA256	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
ECDHE-ECDSA-AES128-SHA	Supported	Supported	Supported	Supported	N/A	Supported	N/A	N/A	Supported
ECDHE-ECDSA-AES256-GCM-SHA384	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
ECDHE-ECDSA-AES256-SHA384	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
ECDHE-ECDSA-AES256-SHA	Supported	Supported	Supported	Supported	N/A	Supported	N/A	N/A	Supported
ECDHE-RSA-AES128-GCM-SHA256	N/A	N/A	N/A	Supported	N/A	Supported	Supported	Supported	Supported
TLS_AES_256_GCM_SHA384	N/A	N/A	N/A	N/A	N/A	Supported	Supported	Supported	N/A
TLS_CHACHA20_POLY1305_SHA256	N/A	N/A	N/A	N/A	N/A	Supported	Supported	Supported	N/A
TLS_AES_128_GCM_SHA256	N/A	N/A	N/A	N/A	N/A	Supported	Supported	Supported	N/A
TLS_AES_128_CCM_8_SHA256	N/A	N/A	N/A	N/A	N/A	Supported	Supported	Supported	N/A

Security Policy	tls-1-0	tls-1-1	tls-1-2	tls-1-0-inherit	tls-1-2-strict	tls-1-0-with-1-3	tls-1-2-fs-with-1-3	tls-1-2-fs	hybrid-policy-1-0
TLS_AES_128_GCM_SHA256	N/A	N/A	N/A	N/A	N/A	Supported	Supported	Supported	N/A
DHE-RSA-AES128-SHA	N/A	N/A	N/A	Supported	N/A	N/A	N/A	N/A	N/A
DHE-DSS-AES128-SHA	N/A	N/A	N/A	Supported	N/A	N/A	N/A	N/A	N/A
CAMELLIA128-SHA	N/A	N/A	N/A	Supported	N/A	N/A	N/A	N/A	N/A
EDH-RSA-DES-CBC3-SHA	N/A	N/A	N/A	Supported	N/A	N/A	N/A	N/A	N/A
DES-CBC3-SHA	N/A	N/A	N/A	Supported	N/A	N/A	N/A	N/A	N/A
ECDHE-RSA-RC4-SHA	N/A	N/A	N/A	Supported	N/A	N/A	N/A	N/A	N/A
RC4-SHA	N/A	N/A	N/A	Supported	N/A	N/A	N/A	N/A	N/A
DHE-RSA-AES256-SHA	N/A	N/A	N/A	Supported	N/A	N/A	N/A	N/A	N/A
DHE-DSS-AES256-SHA	N/A	N/A	N/A	Supported	N/A	N/A	N/A	N/A	N/A
DHE-RSA-CAMELLIA256-SHA	N/A	N/A	N/A	Supported	N/A	N/A	N/A	N/A	N/A
ECC-SM4-SM3	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Supported
ECDHE-SM4-SM3	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Supported

Changing a Security Policy

When you change a security policy, ensure that the security group rules configured for backend servers allow traffic from 100.125.0.0/16 to backend servers and allows ICMP packets for UDP health checks. Otherwise, backend servers will be considered unhealthy, resulting in service interruptions.

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
3. Click **Listeners**, locate the listener, and click its name.
4. On the **Summary** tab, click **Edit** on the top right.
5. In the **Edit** dialog box, expand **Advanced Settings** and change the security policy.
6. Click **OK**.

2.7.4 Access Control

2.7.4.1 What Is Access Control?

Access control allows you to add a whitelist or blacklist to specify IP addresses that are allowed or denied to access a listener.

Whitelist and Blacklist

You can set a whitelist or blacklist to control access to a listener.

- Once the whitelist is set, only the IP addresses or CIDR blocks specified in the IP address group can access the listener.

Access control policies only take effect for new connections, but not for connections that have been established. If a whitelist is configured for a listener but IP addresses that are not in the whitelist can access the backend server associated with the listener, one possible reason is that a persistent connection is established between the client and the backend server. To deny IP addresses that are not in the whitelist from accessing the listener, the persistent connection between the client and the backend server needs to be disconnected.

- Once the blacklist is set, the IP addresses or CIDR blocks specified in the blacklist cannot access the listener.

NOTE

- Access control does not restrict the ping command. You can still ping a load balancer from restricted IP addresses.
- To ping the IP address of a shared load balancer, you need to add a listener and associate a backend server to it.
- Whitelists and blacklists do not conflict with inbound security group rules. Access control defines the IP addresses or CIDR blocks that are allowed or denied to access listeners, while inbound security group rules control access to backend servers. Requests first match the whitelists or blacklists then the security group rules before they finally reach backend servers.

Configuring Access Control

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
3. Configure access control for a listener in either of the following ways:
 - On the **Listeners** page, locate the listener and click **Configure** in the **Access Control** column.
 - Click the name of the target listener. On the **Summary** page, click **Configure** on the right of **Access Control**.
4. In the displayed **Configure Access Control** dialog box, configure parameters as described in [Table 2-37](#).

Table 2-37 Parameter description

Parameter	Description
Access Control	Specifies how access to the listener is controlled. Three options are available: <ul style="list-style-type: none">• All IP addresses: All IP addresses can access the listener.• Whitelist: Only IP addresses in the IP address group can access the listener.• Blacklist: IP addresses in the IP address group are not allowed to access the listener.
IP Address Group	Specifies the IP address group associated with a whitelist or blacklist. If there is no IP address group, create one first. For more information, see What Is an IP Address Group?
Access Control	If you have set Access Control to Whitelist or Blacklist , you can enable or disable access control. <ul style="list-style-type: none">• Only after you enable access control, the whitelist or blacklist takes effect.• If you disable access control, the whitelist or blacklist does not take effect.

5. Click **OK**.

2.7.4.2 IP Address Group

What Is an IP Address Group?

An IP address group allows you to manage a collection of IP addresses that have the same security requirements or whose security requirements change frequently.

If you want to use a whitelist or blacklist for access control, you must select an IP address group.

- **Whitelist:** Only IP addresses in the IP address group can access the listener. If the IP address group does not contain any IP address and you have selected a whitelist for access control, no IP addresses can access the listener.
- **Blacklist:** IP addresses in the IP address group are denied to access the listener. If the IP address group does not contain any IP address and you have selected a blacklist for access control, all IP addresses can access the listener.

Notes and Constraints

- By default, you can create a maximum of 50 IP address groups.
- An IP address group can be associated with a maximum of 50 listeners.

Creating an IP Address Group

1. Go to the [load balancer list page](#).
2. In the navigation pane on the left, choose **Elastic Load Balance > IP Address Groups**.
3. On the displayed page, click **Create IP Address Group**.
4. Configure the parameters based on [Table 2-38](#).

Table 2-38 Parameters required for creating an IP address group

Parameter	Description	Example Value
Name	Specifies the name of the IP address group.	ipGroup-01
Enterprise Project	Specifies an enterprise project by which cloud resources and members are centrally managed. For details, see the Enterprise Management User Guide .	N/A
IP Addresses	Specifies IPv4 or IPv6 IP addresses or CIDR blocks that are added to the whitelist or blacklist for access control. <ul style="list-style-type: none">• Each line must contain an IP address or a CIDR block and end with a line break.• You can add remarks at the end of each IP address or CIDR block and separate them with a vertical bar (). The remarks can be up to 255 characters long. Angle brackets (<>) are not allowed.• You can add a maximum of 300 IP addresses or CIDR blocks in each IP address group.	<ul style="list-style-type: none">• Without remarks: 10.168.2.24• With remarks: 10.168.16.0/24 ECS01

Parameter	Description	Example Value
Description	Provides supplementary information about the IP address group.	N/A

5. Click **OK**.

Managing IP Addresses in an IP Address Group

After an IP address group is created, you can manage the IP addresses in an IP address group as required:

- [Adding IP Addresses](#)
- [Changing IP Addresses](#)
- [Deleting an IP Address](#)

The IP addresses can be in the following formats:

- Each line must contain an IP address or a CIDR block and end with a line break.
- You can add remarks at the end of each IP address or CIDR block and separate them with a vertical bar (|), for example, 192.168.10.10 | ECS01. The remarks can be up to 255 characters long. Angle brackets (<>) are not allowed.
- You can add a maximum of 300 IP addresses or CIDR blocks to each IP address group.

Adding IP Addresses

You can add IP addresses to an existing IP address group.

1. Go to the [load balancer list page](#).
2. In the navigation pane on the left, choose **Elastic Load Balance > IP Address Groups**.
3. On the **IP Address Groups** page, locate the target IP address group and click its name.
4. In the lower part of the displayed page, choose **IP Addresses** tab and click **Add IP Addresses**. On the **Add IP Addresses** page, add IP addresses.
5. Click **OK**.

Changing IP Addresses

You can perform the following steps to change all IP addresses in an IP address group:

1. Go to the [load balancer list page](#).
2. In the navigation pane on the left, choose **Elastic Load Balance > IP Address Groups**.
3. On the **IP Address Groups** page, you can:

- a. Modify the basic information and change IP addresses of an IP address group:
 - i. Locate the target address group, click **Modify** in the **Operation** column. You can modify the name and description of an IP address group, and change all its IP addresses.
 - ii. Click **OK**.
- b. Only change IP addresses:
 - i. Locate the target IP address group and click its name.
 - ii. In the lower part of the displayed page, choose **IP Addresses** tab, click **Change IP Address**, and change IP addresses as you need.
 - iii. Click **OK**.

Deleting an IP Address

If you want to delete IP addresses in batches from an IP address group, see [Changing IP Addresses](#).

To delete an IP address from an IP address group, perform the following operations:

1. Go to the [load balancer list page](#).
2. In the navigation pane on the left, choose **Elastic Load Balance > IP Address Groups**.
3. On the **IP Address Groups** page, locate the target IP address group and click its name.
4. In the IP address list, locate the IP address you want to delete and click **Delete** in the **Operation** column.
5. Confirm the information and click **OK**.

Viewing the Details of an IP Address Group

You can view the details of an IP address group, including:

- Name, ID, and creation time
 - IP addresses and CIDR blocks
 - Associated listeners
1. Go to the [load balancer list page](#).
 2. In the navigation pane on the left, choose **Elastic Load Balance > IP Address Groups**.
 3. On the **IP Address Groups** page, locate the target IP address group and click its name.
 4. Viewing the basic information about the IP address group.
 - a. On the **IP Addresses** tab, view the IP addresses or CIDR blocks.
 - b. On the **Associated Listeners** tab, view the listeners associated with the IP address group.

Deleting an IP Address Group

If an IP address group is used for controlling access to a listener, it cannot be deleted.

You can view the listeners associated with an IP address group by referring to [Viewing the Details of an IP Address Group](#). For details about how to disassociate an IP address group from a listener, see [Configuring Access Control](#).

1. Go to the [load balancer list page](#).
2. In the navigation pane on the left, choose **Elastic Load Balance > IP Address Groups**.
3. On the **IP Address Groups** page, locate the IP address group and click **Delete** in the **Operation** column.
4. Click **OK**.

2.7.5 Certificate

2.7.5.1 Certificate Overview

When you add an HTTPS or TLS listener, you need to bind a server certificate to it. To enable mutual authentication, you also need to bind a CA certificate to the listener. You can purchase a server certificate from Huawei Cloud Cloud Certificate Manager (CCM) or upload your own certificates to the ELB console.

Use Cases

When you add an HTTPS or TLS listener to route requests, you need to select **SSL Authentication**. For one-way authentication, you need to configure a server certificate for the listener. For two-way authentication, you need to configure both a server certificate and a CA certificate.

Table 2-39 SSL authentication

One-way Authentication	Only backend servers will be authenticated. You need to bind a server certificate to the listener to authenticate the server.
Mutual Authentication	The clients and the load balancer authenticate each other. Only authenticated clients will be allowed to access the load balancer. You need to bind both a server certificate and a CA certificate to the listener to allow the clients and the load balancer to authenticate each other. You do not need to configure two-way authentication on the backend servers.

ELB supports two types of certificates.

Table 2-40 Certificate types

Server Certificate	Used for SSL handshake negotiations if an HTTPS or TLS listener is used. Both the certificate content and private key are required.
CA Certificate	Also called client CA public key certificate and used to verify the client certificate issuer. If mutual authentication is required, connections can be established only when the client provides a certificate issued by a specific CA.

Precautions

- A certificate can be used by multiple load balancers but only needs to be uploaded to ELB once.
- You must specify a domain name for an SNI certificate. The domain name must be the same as that in the certificate. An SNI certificate can have multiple domain names.
- For each certificate type, a listener can have only one certificate by default, but a certificate can be bound to more than one listener. If SNI is enabled for the listener, multiple server certificates can be bound.
- Only original certificates are supported. That is to say, you cannot encrypt your certificates.
- You can use self-signed certificates. However, note that self-signed certificates pose security risks. It is recommended that you use certificates issued by third parties.
- ELB only supports certificates in PEM format. If you have a certificate in any other format, you must convert it to a PEM-encoded certificate.
- If a certificate has expired, you need to manually replace or delete it.

Certificate Format

You can copy and paste the certificate body to create a certificate or directly upload a certificate.

A certificate issued by the Root CA is unique, and no additional certificates are required. The configured site is considered trustable by access devices, such as a browser.

The body of the server and CA certificates must meet the requirements as described below.

- The content must start with -----BEGIN CERTIFICATE----- and ends with -----END CERTIFICATE-----.
- Each row contains 64 characters except the last row.
- There are no empty rows.

The following is an example:

```
-----BEGIN CERTIFICATE-----  
Base64-encoded certificate  
-----END CERTIFICATE-----
```

Private Key Format

When creating a server certificate, you also need to upload the private key of the certificate. You can copy and paste the private key content or directly upload the private key in the required format.

Private keys must be unencrypted and meet the following requirements:

- The value must be in PEM format.
 - The content must start with -----BEGIN RSA PRIVATE KEY----- and end with -----END RSA PRIVATE KEY-----.
 - The content must start with -----BEGIN EC PRIVATE KEY----- and end with -----END EC PRIVATE KEY-----.
- There are no empty rows. Each row contains 64 characters except the last row.

The following is an example:

```
-----BEGIN RSA PRIVATE KEY-----  
[key]  
-----END RSA PRIVATE KEY-----
```

Converting Certificate Formats

ELB only supports certificates in PEM format. If you have a certificate in any other format, you must convert it to a PEM-encoded certificate. There are some common methods for converting a certificate from any other format to PEM.

From DER to PEM

The DER format is usually used on a Java platform.

Run the following command to convert the certificate format:

```
openssl x509 -inform der -in certificate.cer -out certificate.pem
```

Run the following command to convert the private key format:

```
openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem
```

From P7B to PEM

The P7B format is usually used by Windows and Tomcat servers.

Run the following command to convert the certificate format:

```
openssl pkcs7 -print_certs -in incertificate.p7b -out outcertificate.cer
```

From PFX to PEM

The PFX format is usually used by Windows servers.

Run the following command to convert the certificate format:

```
openssl pkcs12 -in certname.pfx -nokeys -out cert.pem
```

Run the following command to convert the private key format:

```
openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes
```

2.7.5.2 Adding a Certificate

Scenarios

To enable authentication for securing data transmission over HTTPS, ELB allows you to bind certificates to HTTPS listeners of a load balancer.

- **Server certificate:** You can purchase a certificate from SSL Certificate Manager (SCM) or upload your own certificates.
- **CA certificate:** You can only upload your own CA certificates.
- **Server SM certificate:** You can purchase a certificate from SSL Certificate Manager (SCM) or upload your own certificates.

NOTE

If you want to use the same certificate in two regions, you need to add a certificate in each region.

Adding a Server Certificate



1. Log in to the management console.
2. In the upper left corner of the page, click  and select the desired region and project.
3. Click  in the upper left corner to display **Service List** and choose **Networking > Elastic Load Balance**.
4. In the navigation pane on the left, choose **Certificates**.
5. Click **Add Certificate** on the top right corner and set parameters by referring to [Table 2-41](#).

Table 2-41 Server certificate parameters

Parameter	Description
Certificate Type	<p>Specifies the certificate type. Select Server certificate.</p> <ul style="list-style-type: none">• Server certificate: used for SSL handshake negotiations if an HTTPS listener is used. Both the certificate content and private key are required.• CA certificate: issued by a certificate authority (CA) and used to verify the certificate issuer. If HTTPS mutual authentication is required, HTTPS connections can be established only when the client provides a certificate issued by a specific CA.

Parameter	Description
Source	<p>Specifies the source of a certificate. You can purchase a certificate from CCM or upload your own certificates.</p> <ul style="list-style-type: none">• SSL Certificate Manager: server certificates provided by CCM. You need to buy a certificate or upload your own certificates.• Your certificate: You need to upload the certificate content and private key of your own certificate to the ELB console. <p>NOTE You are advised to use SCM to manage your certificates.</p>
Certificate	<p>This parameter is only available for certificates managed on the CCM console.</p> <p>You can select a certificate managed by CCM.</p>
Certificate Name	<p>Specifies the name of your certificate.</p> <p>This parameter is only available for your certificates.</p>
Enterprise Project	<p>Specifies an enterprise project by which cloud resources and members are centrally managed.</p>
Certificate Content	<p>Specifies the content of a certificate. This parameter is only available for your certificates.</p> <p>The content must be in PEM format.</p> <p>Click Upload and select the certificate to be uploaded. Ensure that your browser is of the latest version.</p> <p>The format of the certificate body is as follows:</p> <pre>-----BEGIN CERTIFICATE----- Base64-encoded certificate -----END CERTIFICATE-----</pre>
Private Key	<p>Specifies the private key of a certificate. This parameter is only available for your certificates.</p> <p>Click Upload and select the private key to be uploaded. Ensure that your browser is of the latest version.</p> <p>The value must be an unencrypted private key. The private key must be in PEM format as follows:</p> <pre>-----BEGIN PRIVATE KEY----- [key] -----END PRIVATE KEY-----</pre>

Parameter	Description
SNI Domain Name (Optional)	<p>The domain name must be specified if the certificate is intended for SNI.</p> <p>A domain name can contain only letters, digits, and hyphens (-) and consist of multiple labels (max. 63 characters each) separated by periods (.). It cannot start or end with a hyphen (-).</p> <p>You can specify up to 100 domain names, separated by commas (,). A domain name can contain a maximum of 100 characters, and the total length cannot exceed 10,000 characters.</p>
Description	(Optional) Provides supplementary information about the certificate.

Adding a CA Certificate



1. Log in to the management console.
2. In the upper left corner of the page, click  and select the desired region and project.
3. Click  in the upper left corner to display **Service List** and choose **Networking > Elastic Load Balance**.
4. In the navigation pane on the left, choose **Certificates**.
5. Click **Add Certificate** on the top right corner and set parameters by referring to [Table 2-42](#).

Table 2-42 CA certificate parameters

Parameter	Description
Certificate Type	<p>Specifies the certificate type. Select CA certificate.</p> <ul style="list-style-type: none">• Server certificate: used for SSL handshake negotiations if an HTTPS listener is used. Both the certificate content and private key are required.• CA certificate: issued by a certificate authority (CA) and used to verify the certificate issuer. If HTTPS mutual authentication is required, HTTPS connections can be established only when the client provides a certificate issued by a specific CA.
Certificate Name	Specifies the name of the CA certificate.
Enterprise Project	Specifies an enterprise project by which cloud resources and members are centrally managed.

Parameter	Description
Certificate Content	The content must be in PEM format. Click Upload and select the certificate to be uploaded. Ensure that your browser is the latest version. The format of the certificate body is as follows: -----BEGIN CERTIFICATE----- Base64-encoded certificate -----END CERTIFICATE-----
Description	(Optional) Provides supplementary information about the certificate.

6. Click **OK**.

2.7.5.3 Managing Certificates

Scenarios

You can manage your certificates on the ELB console. If a certificate is no longer needed, you can delete it.

Notes and Constraints

A certificate that has been bound to an HTTPS listener cannot be deleted. Disassociate the certificate from the listener first by referring to [Replacing a Certificate](#).

Querying Listeners by Certificate

1. Go to the [load balancer list page](#).
2. In the navigation pane on the left, choose **Certificates**.
3. In the certificate list, click the listener name in the **Listener (Frontend Protocol/Port)** column to view its details.

If there are more than 5 listeners, no listener is displayed in the **Listener (Frontend Protocol/Port)** column. Click **View All**. On the displayed page, click **Listeners**, locate the listener, and click its name to view its details.

Modifying a Certificate

1. Go to the [load balancer list page](#).
2. In the navigation pane on the left, choose **Certificates**.
3. Locate the certificate and click **Modify** in the **Operation** column.
4. In the **Modify Certificate** dialog box, modify the parameters as required.
5. Confirm the information and click **OK**.

Deleting a Certificate

1. Go to the [load balancer list page](#).

2. In the navigation pane on the left, choose **Certificates**.
3. Locate the certificate and click **Delete** in the **Operation** column.
4. In the displayed dialog box, click **OK**.

2.7.5.4 Binding or Replacing a Certificate

Scenarios

You need to bind a certificate when you add an HTTPS listener to a load balancer. If the certificate used by a listener has expired or needs to be replaced due to other reasons, you can replace the certificate on the **Listeners** tab.

If the certificate is also used by other services such as WAF, replace the certificate on all these services to prevent service unavailability.

NOTE

Replacing a certificate and private keys does not affect your applications.

Notes and Constraints

- Only HTTPS listeners require certificates.
- If a certificate has expired, you need to manually replace or delete it.
- The new certificate takes effect immediately. The old certificate is used for established connections, and the new one is used for new connections.

Prerequisites

You have added a certificate by following the instructions in [Adding a Certificate](#).

Binding a Certificate

You can bind certificates when you add an HTTPS listener. For details, see [Adding an HTTPS Listener](#).

Replacing a Certificate

1. Go to the [load balancer list page](#).
2. On the displayed page, locate the load balancer and click its name.
3. Click the **Listeners** tab, locate the listener, and click **Edit** in **Operation** column.
4. On the displayed dialog box, select a server certificate or CA certificate.
5. Click **OK** in the **Edit** dialog box.

2.7.5.5 Replacing the Certificate Bound to Different Listeners

Scenario

If the certificate that is bound to different listeners has expired or needs to be replaced due to other reasons, you can replace the certificate by modifying it on the **Certificates** page.

 **NOTE**

Replacing the certificate and private keys does not affect your applications.

Notes and Constraints

- Only HTTPS and QUIC listeners require certificates.
- The new certificate takes effect immediately. The previous certificate is used for established connections, and the new one is used for new connections.
- SSL Certificate Manager (SCM) allows you to purchase a certificate from Huawei Cloud or upload your own certificates for easier management.

Modifying a Certificate

1. Go to the [load balancer list page](#).
2. In the navigation pane on the left, choose **Certificates**.
3. Locate the certificate and click **Modify** in the **Operation** column.
4. Modify the parameters as required.
5. Confirm the information and click **OK**.

2.7.6 Protection for Mission-Critical Operations

Scenarios

ELB supports sensitive operation protection. When you perform sensitive operations on the management console, you need to enter a credential that can prove your identity. You can perform corresponding operations only after your identity is authenticated. It is recommended that you enable operation protection to secure your account.

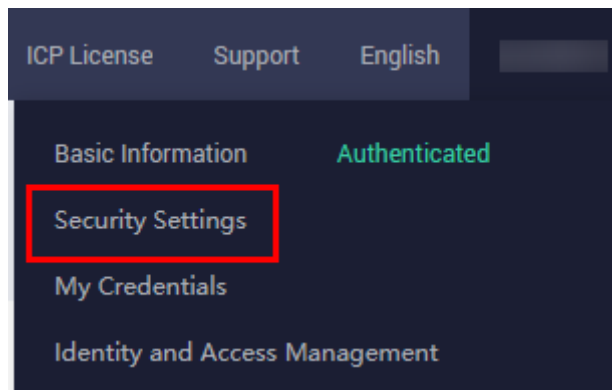
This function can be configured only by the administrator and takes effect for the resources in your account and the resources of users under your account. Common users have only the view permissions. To modify the permissions, contact the administrator.

Enabling Operation Protection

Operation protection is disabled by default. Perform the following operations to enable it:

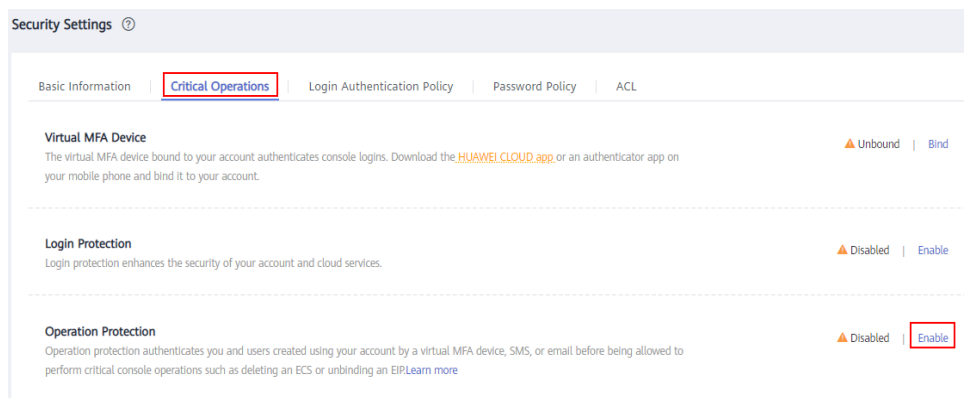
1. Log in to the management console.
2. Move the cursor to the username in the upper right corner of the page and select **Security Settings** from the list.

Figure 2-16 Security settings



3. On the **Security Settings** page, choose **Critical Operations > Operation Protection > Enable**.

Figure 2-17 Critical operations



4. On the **Operation Protection** page, select **Enable**.
If operation protection is enabled, you and IAM users created using your account need to enter a verification code when performing a critical operation, such as deleting an ECS resource.

NOTE

- When performing a critical operation, you will be asked to choose a verification method from email, SMS, and virtual MFA device.
 - If you have bound only a mobile number, only SMS verification is available.
 - If you have bound only an email address, only email verification is available.
 - If you have not bound an email address, mobile number, or virtual MFA device, bind one to perform critical operations.
- You can change the mobile number, email address, and virtual MFA device on the **Basic Information** page.

Verifying Operation Protection

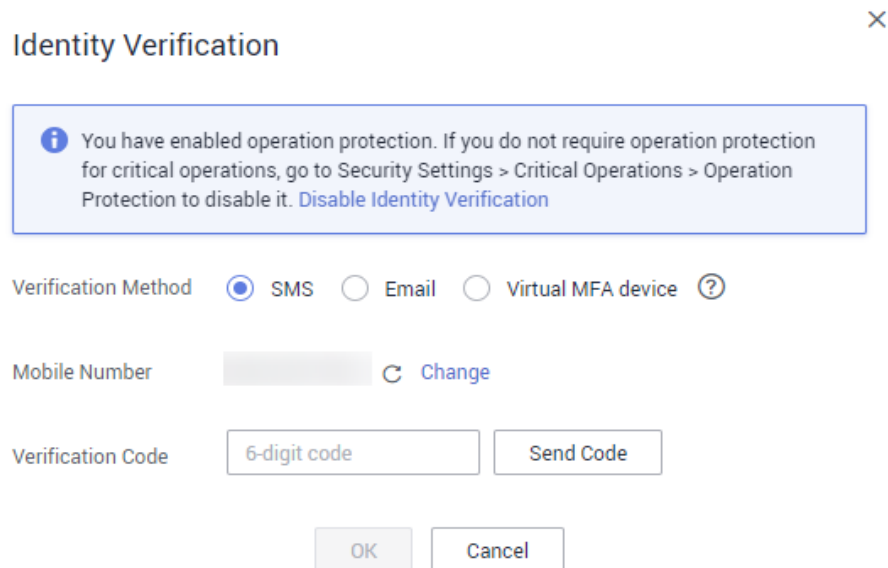
After operation protection is enabled, when you perform a mission-critical operation, the system will verify your identity.

- If you have bound an email address, enter the email verification code.
- If you have bound a mobile number, enter the SMS verification code.

- If you have bound a virtual MFA device, enter a 6-digit dynamic verification code of the MFA device.

When you attempt to delete a load balancer, the following dialog box is displayed, and you need to select a verification method:

Figure 2-18 Identity verification

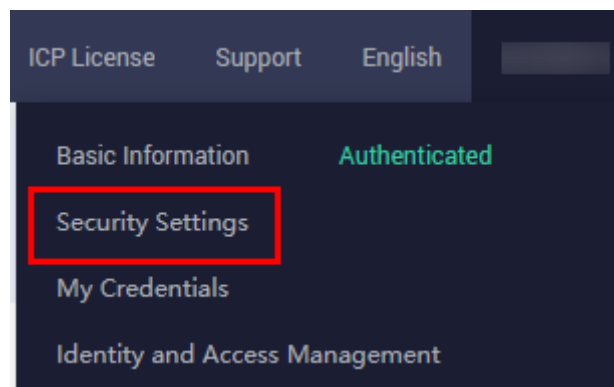


Disabling Operation Protection

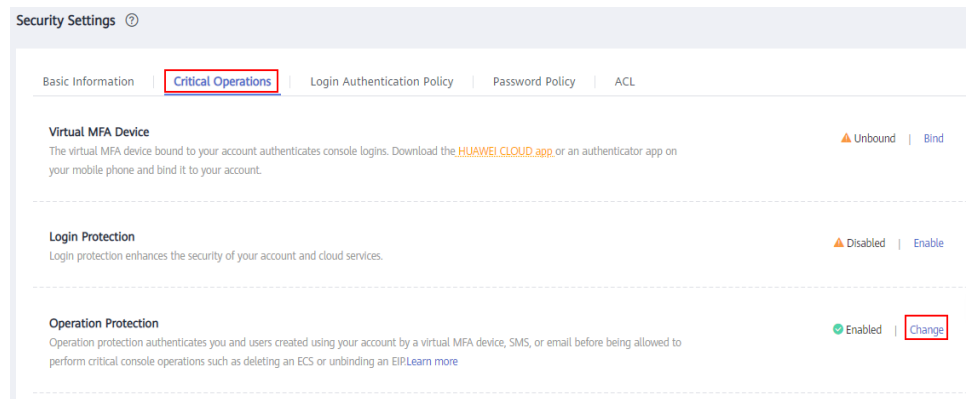
Perform the following operations to disable operation protection:

1. Log in to the management console.
2. Move the cursor to the username in the upper right corner of the page and select **Security Settings** from the list.

Figure 2-19 Security settings



3. On the **Security Settings** page, choose **Critical Operations > Operation Protection > Change**.

Figure 2-20 Modifying operation protection settings

4. On the **Operation Protection** page, select **Disable** and click **OK**.

References

- [How Do I Bind a Virtual MFA Device?](#)
- [How Do I Obtain an MFA Verification Code?](#)

2.8 Access Logging

Scenarios

ELB logs HTTP and HTTPS requests received by shared load balancers, including the time when the request was sent, client IP address, request path, and server response.

With Log Tank Service (LTS), you can view logs of requests to load balancers at Layer 7 and analyze response status codes to quickly locate unhealthy backend servers.

NOTE

ELB displays operations data, such as access logs, on the LTS console. Do not transmit private or sensitive data through fields in access logs. Encrypt your sensitive data if necessary.

Constraints

- Access logging can be configured only for shared load balancers that have HTTP or HTTPS listeners.
- The access logs do not contain requests whose return code is **400 Bad Request**. This is because such requests do not comply with HTTP specification and cannot be processed properly.

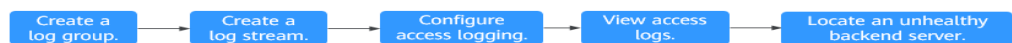
Prerequisites

- You have created an application load balancer. For details, see [Creating a Shared Load Balancer](#).
- You have enabled LTS. For details, see [Accessing LTS](#).

- You have created a backend server group, added backend servers to the group, and deployed services on the backend servers. For details, see [Creating a Backend Server Group](#).
- You have added an HTTP or HTTPS listener to the load balancer. For details, see [Adding an HTTP Listener](#) or [Adding an HTTPS Listener](#).

Flowchart

Figure 2-21 Process for locating an unhealthy backend server



Creating a Log Group



1. Log in to the management console.
2. In the upper left corner of the page, click  and select the desired region and project.
3. Click  in the upper left corner and choose **Management & Governance > Log Tank Service**.
4. In the navigation pane on the left, choose **Log Management**.
5. On the lower part of the displayed page, click **Create Log Group**. In the displayed dialog box, enter a name for the log group.

Figure 2-22 Creating a log group

Create Log Group ×

Log Group Name:
The log group name cannot be the same as the name or original name of another log group.

Enterprise Project Name: C
[View Enterprise Projects](#)

Log Retention Duration:
You can set the retention duration to 1-365 days (30 days by default). Logs older than the specified duration will be automatically deleted. For long-term storage, you can transfer logs to OBS buckets. [SQL analysis is an open beta test \(OBT\) feature and supports only SQL analysis of data generated within 30 days.](#)
You can create log groups for free, but charges apply for log read/write, indexing, and storage. [Pricing details](#)

Tag:

i The log group tag is independent of the log stream tag unless you enable Apply to Log Stream. (Applied once each time) [Learn more](#)

Key	Value	Apply to Log Stream	Operation
+ Add Tags <small>You can add 20 more tags. (System tags not included)</small>			

Remark:

0/1024

6. Confirm the settings and click **OK**.

Creating a Log Stream


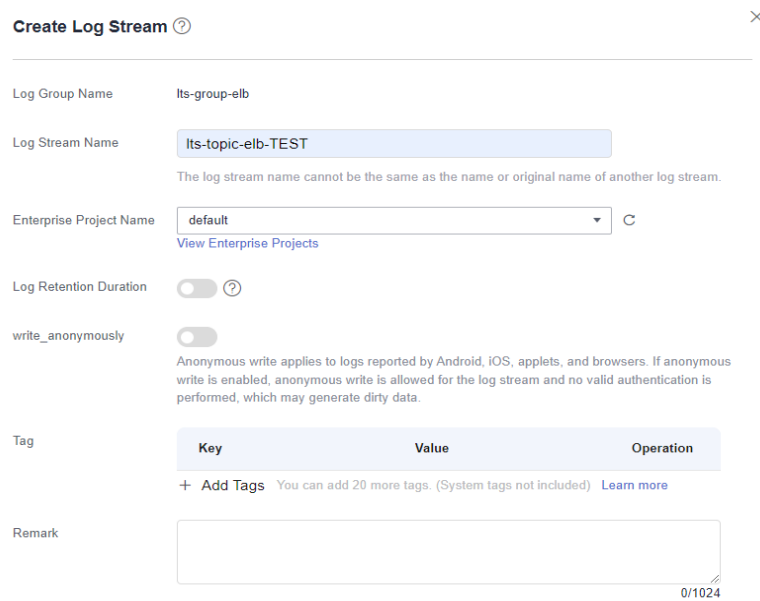
1. On the LTS console, click  on the left of the target log group.
2. Click **Create Log Stream**. In the displayed dialog box, enter a name for the log stream.

Figure 2-23 Creating a log stream



Create Log Stream ? ×

Log Group Name: Its-group-elb

Log Stream Name: Its-topic-elb-TEST
The log stream name cannot be the same as the name or original name of another log stream.

Enterprise Project Name: default C
[View Enterprise Projects](#)

Log Retention Duration: ?

write_anonymously:
Anonymous write applies to logs reported by Android, iOS, applets, and browsers. If anonymous write is enabled, anonymous write is allowed for the log stream and no valid authentication is performed, which may generate dirty data.

Key	Value	Operation
+ Add Tags You can add 20 more tags. (System tags not included) Learn more		

Remark: 0/1024

3. Confirm the settings and click **OK**.

Configuring Access Logging


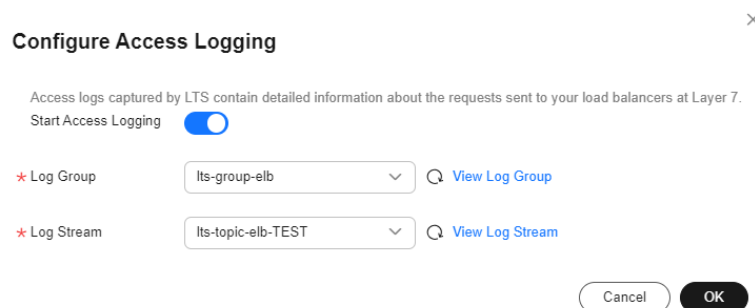
1. Click  in the upper left corner to display **Service List** and choose **Networking > Elastic Load Balance**.
2. On the **Load Balancers** page, locate the load balancer and click its name.
3. Under **Access Logs**, click **Configure Access Logging**.
4. Enable access logging and select the log group and log stream you have created.

Figure 2-24 Configuring access logging



Configure Access Logging ×

Access logs captured by LTS contain detailed information about the requests sent to your load balancers at Layer 7.

Start Access Logging:

* Log Group: Its-group-elb Q [View Log Group](#)

* Log Stream: Its-topic-elb-TEST Q [View Log Stream](#)

5. Click **OK**.

NOTICE

Ensure that the log group is in the same region as the load balancer.

Viewing Access Logs

You can view details about access logs on the:

- ELB console: Click the name of the load balancer and click **Access Logs** to view logs.
- (Recommended) LTS console: Locate the target log group and click its name. On the displayed page, locate the target log stream and click **Real-Time Logs** tab.

The log format is as follows, which cannot be modified:

```
$msec $access_log_topic_id [$time_iso8601] $log_ver $remote_addr:$remote_port $status  
"$request_method $scheme://$host$routier_request_uri $server_protocol" $request_length $bytes_sent  
$body_bytes_sent $request_time "$upstream_status" "$upstream_connect_time" "$upstream_header_time"  
"$upstream_response_time" "$upstream_addr" "$http_user_agent" "$http_referer" "$http_x_forwarded_for"  
$lb_name $listener_name $listener_id  
$pool_name "$member_name" $tenant_id $eip_address:$eip_port "$upstream_addr_priv" $certificate_id  
$ssl_protocol $ssl_cipher $sni_domain_name $tcpinfo_rtt $self_defined_header
```

The following is a log example:

```
1644819836.370 eb11c5a9-93a7-4c48-80fc-03f61f638595 [2022-02-14T14:23:56+08:00] elb_01  
192.168.1.1:888 200 "POST https://www.test.com/example/ HTTP/1.1" 1411 251 3 0.011 "200" "0.000"  
"0.011" "0.011" "100.64.0.129:8080" "okhttp/3.13.1" "-" "-"  
loadbalancer_295a7eee-9999-46ed-9fad-32a62ff0a687 listener_20679192-8888-4e62-a814-a2f870f62148  
3333fd44fe3b42cbaa1dc2c641994d90 pool_89547549-6666-446e-9dbc-e3a551034c46 "-"  
f2bc165ad9b4483a9b17762da851bbbb 121.64.212.1:443 "10.1.1.2:8080" - TLSv1.2 ECDHE-RSA-AES256-  
GCM-SHA384 www.test.com 56704 -
```

Table 2-43 describes the fields in the log.

Table 2-43 Parameter description

Parameter	Description	Value Description	Example Value
msec	Time when the log is written, in seconds with a milliseconds resolution.	Floating-point data	1644819836.370
access_log_topic_id	Log stream ID.	uuid	eb11c5a9-93a7-4c48-80fc-03f61f638595
time_iso8601	Local time in the ISO 8601 standard format.	N/A	[2022-02-14T14:23:56+08:00]

Parameter	Description	Value Description	Example Value
log_ver	Log format version.	Fixed value: elb_01	elb_01
remote_addr: remote_port	IP address and port number of the client.	Records the IP address and port of the client.	192.168.1.1:888
status	HTTP status code.	Records the request status code.	200
request_method scheme://host request_uri server_protocol	Request method. Protocol:// <i>Host name: Request URI Request protocol.</i>	<ul style="list-style-type: none">● request_method: request method.● scheme: HTTP or HTTPS● host: host name, which can be a domain name or an IP address.● request_uri: indicates the native URI initiated by the browser without any modification and it does not include the protocol and host name.	"POST https://www.test.com/example/ HTTP/1.1"
request_length	Length of the request received from the client, including the header and body.	Integer	1411
bytes_sent	Number of bytes sent to the client.	Integer	251
body_bytes_sent	Number of bytes sent to the client (excluding the response header).	Integer	3

Parameter	Description	Value Description	Example Value
request_time	Request processing time in seconds from the time when the load balancer receives the first request packet from the client to the time when the load balancer sends the response packet.	Floating-point data	0.011
upstream_status	HTTP status code returned by the upstream server. <ul style="list-style-type: none">• When the load balancer attempts to retry a request, there will be multiple HTTP status codes.• If the request is not correctly routed to the backend server, a hyphen (-) is displayed as a null value for this field.	HTTP status code returned by the backend server to the load balancer	"200"

Parameter	Description	Value Description	Example Value
upstream_connect_time	<p>Time taken to establish a connection with the server, in seconds, with a milliseconds resolution.</p> <ul style="list-style-type: none">• When the load balancer attempts to retry a request, there will be multiple connection times.• If the request is not correctly routed to the backend server, a hyphen (-) is displayed as a null value for this field.	Floating-point data	"0.000"
upstream_header_time	<p>Time taken to receive the response header from the server, in seconds, with a milliseconds resolution.</p> <ul style="list-style-type: none">• When the load balancer attempts to retry a request, there will be multiple response times.• If the request is not correctly routed to the backend server, a hyphen (-) is displayed as a null value for this field.	Floating-point data	"0.011"

Parameter	Description	Value Description	Example Value
upstream_response_time	<p>Time taken to receive the response from the server, in seconds, with a milliseconds resolution.</p> <ul style="list-style-type: none">• When the load balancer attempts to retry a request, there will be multiple response times.• If the request is not correctly routed to the backend server, a hyphen (-) is displayed as a null value for this field.	Floating-point data	"0.011"
upstream_addr	<p>IP address and port number of the backend server. There may be multiple values separated by commas and spaces, and each value is in the format of <i>{IP address}:{Port number}</i> or <i>-</i>.</p>	IP address and port number	"100.64.0.129:8080" (used by shared load balancers for internal communications)
http_user_agent	<p>http_user_agent in the request header received by the load balancer, indicating the system model and browser information of the client.</p>	Records the browser-related information.	"okhttp/3.13.1"
http_referer	<p>http_referer in the request header received by the load balancer, indicating the page link of the request.</p>	Request for a page link	"-"

Parameter	Description	Value Description	Example Value
http_x_forwarded_for	http_x_forwarded_for in the request header received by the load balancer, indicating the IP address of the proxy server that the request passes through.	IP address	"-"
lb_name	Load balancer name in the format of loadbalancer_load balancer ID	String	loadbalancer_295a7eee-9999-46ed-9fad-32a62ff0a687
listener_name	Listener name in the format of listener_listener ID .	String	listener_20679192-8888-4e62-a814-a2f870f62148
listener_id	Listener ID. This field can be ignored.	String	3333fd44fe3b42cbaa1dc2c641994d90
pool_name	Backend server group name in the format of pool_backend server group ID	String	pool_89547549-6666-446e-9dbc-e3a551034c46
member_name	Backend server name in the format of member_server ID . This field is not supported yet. There may be multiple values separated by commas and spaces, and each value is a member ID (member_id) or "-".	String	"-"
tenant_id	Tenant ID.	String	f2bc165ad9b4483a9b17762da851bbbb

Parameter	Description	Value Description	Example Value
eip_address:eip_port	EIP of the load balancer and frontend port that were set when the listener was added.	EIP of the load balancer and frontend port that were set when the listener was added.	121.64.212.1:443
upstream_addr_priv	IP address and port number of the backend server. There may be multiple values separated by commas and spaces, and each value is in the format of <i>{IP address}:{Port number}</i> or <i>-</i> .	IP address and port number	"10.1.1.2:8080"
certificate_id	[HTTPS listener] Certificate ID used for establishing an SSL connection. This field is not supported yet.	String	N/A
ssl_protocol	[HTTPS listener] Protocol used for establishing an SSL connection. For a non-HTTPS listener, a hyphen (-) is displayed as a null value for this field.	String	TLSv1.2
ssl_cipher	[HTTPS listener] Cipher suite used for establishing an SSL connection. For a non-HTTPS listener, a hyphen (-) is displayed as a null value for this field.	String	ECDHE-RSA-AES256-GCM-SHA384

Parameter	Description	Value Description	Example Value
sni_domain_name	[HTTPS listener] SNI domain name provided by the client during SSL handshakes. For a non-HTTPS listener, a hyphen (-) is displayed as a null value for this field.	String	www.test.com
tcpinfo_rtt	TCP Round Trip Time (RTT) between the load balancer and client in microseconds.	Integer	56704
self_defined_header	This field is reserved. The default value is -.	String	N/A

Log analysis

At 14:23:56 GMT+08:00 on Feb 14, 2022, the load balancer receives an HTTP/1.1 POST request from a client whose IP address and port number are 192.168.1.1 and 888, then routes the request to a backend server whose IP address and port number are 100.64.0.129 and 8080, and finally returns 200 OK to the client after receiving the status code from the backend server.

Analysis results:

The backend server responds to the request normally.

Configuring Log Transfer

If you want to analyze access logs later, transfer the logs to OBS or Data Ingestion Service (DIS) for storage.



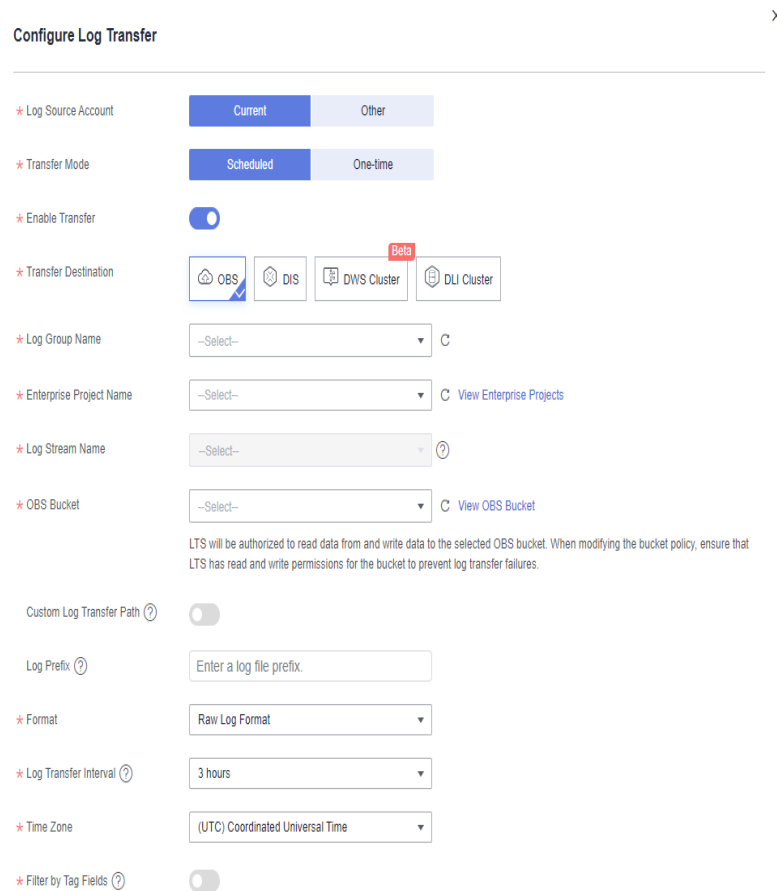
1. Log in to the management console.
2. In the upper left corner of the page, click  and select the desired region and project.
3. Click  in the upper left corner and **Management & Governance > Log Tank Service**.
4. In the navigation pane on the left, choose **Log Transfer**.
5. On the **Log Transfer** page, click **Configure Log Transfer** in the upper right corner.

Figure 2-25 Configuring log transfer

Configure Log Transfer

* Log Source Account: Current | Other

* Transfer Mode: Scheduled | One-time

* Enable Transfer:

* Transfer Destination: OBS | DIS | DWS Cluster | DLI Cluster

* Log Group Name: --Select--

* Enterprise Project Name: --Select-- View Enterprise Projects

* Log Stream Name: --Select--

* OBS Bucket: --Select-- View OBS Bucket

LTS will be authorized to read data from and write data to the selected OBS bucket. When modifying the bucket policy, ensure that LTS has read and write permissions for the bucket to prevent log transfer failures.

Custom Log Transfer Path:

Log Prefix: Enter a log file prefix.

* Format: Raw Log Format

* Log Transfer Interval: 3 hours

* Time Zone: (UTC) Coordinated Universal Time

* Filter by Tag Fields:

6. Configure the parameters. For details, see the [Log Tank Service User Guide](#).

2.9 Tags and Quotas

2.9.1 Tag



Scenarios

If you have a large number of cloud resources, you can add different tags to the resources to quickly identify them and use these tags to easily manage your resources.

Adding a Tag to a Load Balancer

You can add a tag to a load balancer in the following methods:

- Add a tag when you create a load balancer.
For details, see [Creating a Shared Load Balancer](#).
- Add a tag to an existing load balancer.
 - a. Log in to the management console.



- b. In the upper left corner of the page, click  and select the desired region and project.
- c. Click  in the upper left corner to display **Service List** and choose **Networking > Elastic Load Balance**.
- d. On the **Load Balancers** page, locate the load balancer and click its name.
- e. Under **Tags**, click **Add Tag**.
- f. In the **Add Tag** dialog box, enter a tag key and value and click **OK**.

 **NOTE**

- A maximum of 20 tags can be added to a load balancer.
- Each tag is a key-value pair, and the tag key is unique.

Adding a Tag to a Listener



To add a tag to an existing listener, perform the following steps:

1. Log in to the management console.
2. In the upper left corner of the page, click  and select the desired region and project.
3. Click  in the upper left corner to display **Service List** and choose **Networking > Elastic Load Balance**.
4. On the **Load Balancers** page, locate the load balancer and click its name.
5. Click **Listeners**, locate the listener, and click its name.
6. Under **Tags**, click **Add Tag**.
7. In the **Add Tag** dialog box, enter a tag key and value and click **OK**.

 **NOTE**

- A maximum of 20 tags can be added to a listener.
- Each tag is a key-value pair, and the tag key is unique.

Modifying a Tag of a Load Balancer

1. Log in to the management console.
2. In the upper left corner of the page, click  and select the desired region and project.
3. Click  in the upper left corner to display **Service List** and choose **Networking > Elastic Load Balance**.
4. On the **Load Balancers** page, locate the load balancer and click its name.
5. Click **Tags**, select the tag to be edited, and click **Edit** in the **Operation** column. In the **Edit Tag** dialog box, enter a tag value.



 **NOTE**

The tag key cannot be changed.

6. In the **Add Tag** dialog box, enter a tag key and value and click **OK**.

The operations for modifying a listener tag are not detailed here. Refer to the operations of modifying a load balancer tag.

Deleting a Tag from a Load Balancer

1. Log in to the management console.
2. In the upper left corner of the page, click  and select the desired region and project.
3. Click  in the upper left corner to display **Service List** and choose **Networking > Elastic Load Balance**.
4. On the **Load Balancers** page, locate the load balancer and click its name.
5. Click **Tags**, select the tag to be deleted, and click **Delete** in the **Operation** column.
6. In the displayed dialog box, click **OK**.

The operations for deleting a listener tag are not detailed here. Refer to the operations of deleting a load balancer tag.

2.9.2 Quotas

What Is Quota?

Quotas can limit the number of resources available to users, such as the maximum number of ECSs or EVS disks that can be created.

If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

How Do I View My Quotas?


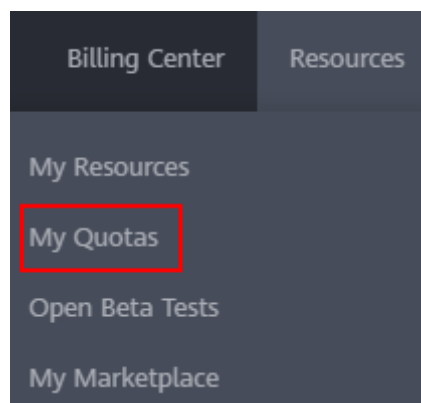
1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, choose **Resources > My Quotas**.
The **Service Quota** page is displayed.

Figure 2-26 My Quotas

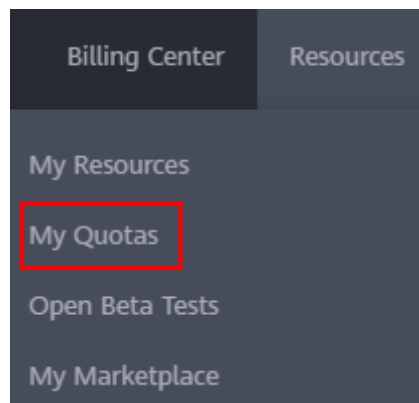


4. View the used and total quota of each type of resources on the displayed page.
If a quota cannot meet service requirements, apply for a higher quota.

How Do I Apply for a Higher Quota?

1. Log in to the management console.
2. In the upper right corner of the page, choose **Resources > My Quotas**.
The **Quotas** page is displayed.

Figure 2-27 My quotas



3. Click **Increase Quota** in the upper right corner of the page.

Figure 2-28 Increasing quota

Service	Resource Type	Used Quota	Total Quota
Auto Scaling	AS group	0	
	AS configuration	0	
Image Management Service	Image	0	
	Cluster	0	
FunctionGraph	Function	0	
	Code storage(MB)	0	
Elastic Volume Service	Disk	3	
	Disk capacity(GB)	120	
Storage Disaster Recovery Service	Snapshots	4	
	Protection group	0	
Cloud Server Backup Service	Replication pair	0	
	Backup Capacity(GB)	0	
Scalable File Service	Backup	0	
	File system	0	
CDN	File system capacity(GB)	0	
	Domain name	0	
	File URL refreshing	0	
	Directory URL refreshing	0	
	URL refreshing	0	

4. On the **Create Service Ticket** page, configure parameters as required.
In the **Problem Description** area, fill in the content and reason for adjustment.
5. After all necessary parameters are configured, select **I have read and agree to the Ticket Service Protocol and Privacy Statement** and click **Submit**.

2.10 Cloud Eye Monitoring

2.10.1 Monitoring ELB Resources

Scenarios

Cloud Eye is a multi-dimensional resource monitoring service. You can use Cloud Eye to monitor ELB resources in real time, set alarm rules, identify resource exceptions, and quickly respond to resource changes.

Cloud Eye is enabled automatically after you create a load balancer. For more information about Cloud Eye, see [What Is Cloud Eye?](#)

Setting an Alarm Rule



You can set alarm rules on the Cloud Eye console to send you notifications in case of exceptions.

For details about how to set alarm rules, see [Creating an Alarm Rule](#).

Viewing Monitoring Metrics


You can view the metrics described in [Monitoring Metrics](#) either on the ELB console or on the Cloud Eye console.


Viewing Monitoring Metrics on the ELB Console

1. Log in to the management console.
2. In the upper left corner of the page, click  and select the desired region and project.
3. Click  in the upper left corner to display **Service List** and choose **Networking > Elastic Load Balance**.
4. On the **Load Balancers** page, locate the load balancer and click its name.
5. View the metrics of each load balancer and listener.
 - a. Load balancer: Click the **Monitoring** tab and select **Load balancer for Dimension**.
 - b. Listener (two ways):
 - i. Click the **Monitoring** tab, select **Listener for Dimension**, select the target listener, and view the monitoring metrics.
 - ii. Click the **Listeners** tab, locate the target listener, and click its name. Switch to the **Monitoring** tab and view the monitoring metrics.

Viewing Monitoring Metrics on the Cloud Eye Console

For details about how to view load balancer monitoring metrics on the Cloud Eye console, see [Querying Metrics of a Cloud Service](#).

1. Log in to the management console.
2. In the upper left corner of the page, click  and select the desired region and project.

3. Click  in the upper left corner and choose **Management & Governance > Cloud Eye**.
4. In the navigation pane on the left, choose **Cloud Service Monitoring**. In the displayed page, locate the **Dashboard** column and click **Elastic Load Balance ELB**.
5. On the displayed page, locate the target load balancer and click its name. Alternatively, locate the load balancer and click **View Metric** in the **Operation** column.
6. Select the time period during which you want to view metrics. You can select a system-defined time period (for example, last 1 hour) or specify a time period.
7. Click **Select Metric** in the upper right corner and select the metrics to be viewed.

2.10.2 Monitoring Metrics

Overview

This section describes the namespace, the metrics that can be monitored by Cloud Eye, and dimensions of these metrics. You can view the [metrics reported by ELB and the generated alarms](#) on the Cloud Eye console.

Namespace

SYS.ELB

Load Balancer Metrics

For shared load balancers, you can view the monitoring metrics by load balancer or listener.

Table 2-44 Metrics supported by each shared load balancer

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
m1_cps	Concurrent Connections	Load balancing at Layer 4: total number of TCP and UDP connections from the monitored object to backend servers. Load balancing at Layer 7: total number of TCP connections from the clients to the monitored object. Unit: Count	≥ 0	Shared load balancer	1 minute
m2_act_conn	Active Connections	Number of TCP and UDP connections in the ESTABLISHED state between the monitored object and backend servers. You can run the following command to view the connections (both Windows and Linux servers): netstat -an Unit: Count	≥ 0	Shared load balancer	1 minute
m3_inact_conn	Inactive Connections	Number of TCP connections between the monitored object and backend servers except those in the ESTABLISHED state. You can run the following command to view the connections (both Windows and Linux servers): netstat -an Unit: Count	≥ 0	Shared load balancer	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
m4_ncps	New Connections	Number of connections established between clients and the monitored object per second. Unit: Count/s	$\geq 0/s$	Shared load balancer	1 minute
m5_in_pps	Incoming Packets	Number of packets received by the monitored object per second. Unit: Count/s	$\geq 0/s$	Shared load balancer	1 minute
m6_out_pps	Outgoing Packets	Number of packets sent from the monitored object per second. Unit: Count/s	$\geq 0/s$	Shared load balancer	1 minute
m7_in_Bps	Inbound Rate	Traffic used for accessing the monitored object from the Internet. Unit: bytes/s	≥ 0 byte/s	Shared load balancer	1 minute
m8_out_Bps	Outbound Rate	Traffic used by the monitored object to access the Internet per second. Unit: bytes/s	≥ 0 byte/s	Shared load balancer	1 minute
m9_abnormal_servers	Unhealthy Servers	Number of unhealthy backend servers associated with the monitored object. Unit: Count	≥ 0	Shared load balancer	1 minute
ma_normal_servers	Healthy Servers	Number of healthy backend servers associated with the monitored object. Unit: Count	≥ 0	Shared load balancer	1 minute
m22_in_bandwidth	Inbound Bandwidth	Bandwidth used for accessing the monitored object from the Internet. Unit: bits/s	≥ 0 bit/s	Shared load balancer	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
m23_out_bandwidth	Outbound Bandwidth	Bandwidth used by the monitored object to access the Internet. Unit: bits/s	≥ 0 bit/s	Shared load balancer	1 minute
m1e_server_rps	Reset Packets from Backend Servers	Number of reset packets sent from backend servers to clients. These reset packets are generated by the backend servers and then forwarded by the load balancer. This metric is available only for TCP listeners. Unit: Count/s	≥ 0 /s	Shared load balancer	1 minute
m21_client_rps	Reset Packets from Clients	Number of reset packets sent by clients to backend servers. These reset packets are generated by clients and then forwarded by the load balancer. This metric is available only for TCP listeners. Unit: Count/s	≥ 0 /s	Shared load balancer	1 minute
m1f_lvs_rps	Reset Packets from Load Balancers	Number of reset packets generated by the load balancer. This metric is available only for TCP listeners. Unit: Count/s	≥ 0 /s	Shared load balancer	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
mb_l7_queries	Layer-7 Query Rate	Number of requests the monitored object receives per second. This metric is available only when the frontend protocol is HTTP or HTTPS. Unit: Count/s	$\geq 0/s$	Shared load balancer	1 minute
mc_l7_http_2xx	Layer-7 2xx Status Codes	Number of 2xx status codes returned by the load balancer and backend servers. This metric is available only when the frontend protocol is HTTP or HTTPS. Unit: Count/s	$\geq 0/s$	Shared load balancer	1 minute
md_l7_http_3xx	Layer-7 3xx Status Codes	Number of 3xx status codes returned by the load balancer and backend servers. This metric is available only when the frontend protocol is HTTP or HTTPS. Unit: Count/s	$\geq 0/s$	Shared load balancer	1 minute
me_l7_http_4xx	Layer-7 4xx Status Codes	Number of 4xx status codes returned by the load balancer and backend servers. This metric is available only when the frontend protocol is HTTP or HTTPS. Unit: Count/s	$\geq 0/s$	Shared load balancer	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
mf_l7_http_5xx	Layer-7 5xx Status Codes	Number of 5xx status codes returned by the load balancer and backend servers. This metric is available only when the frontend protocol is HTTP or HTTPS. Unit: Count/s	$\geq 0/s$	Shared load balancer	1 minute
m10_l7_http_other_status	Layer-7 Other Status Codes	Number of status codes returned by the load balancer and backend servers except 2xx, 3xx, 4xx, and 5xx status codes. This metric is available only when the frontend protocol is HTTP or HTTPS. Unit: Count/s	$\geq 0/s$	Shared load balancer	1 minute
m11_l7_http_404	Layer-7 404 Not Found	Number of 404 Not Found status codes returned by the load balancer and backend servers. This metric is available only when the frontend protocol is HTTP or HTTPS. Unit: Count/s	$\geq 0/s$	Shared load balancer	1 minute
m12_l7_http_499	Layer-7 499 Client Closed Request	Number of 499 Client Closed Request status codes returned by the load balancer and backend servers. This metric is available only when the frontend protocol is HTTP or HTTPS. Unit: Count/s	$\geq 0/s$	Shared load balancer	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
m13_l7_http_502	Layer-7 502 Bad Gateway	<p>Number of 502 Bad Gateway status codes returned by the load balancer and backend servers.</p> <p>This metric is available only when the frontend protocol is HTTP or HTTPS.</p> <p>Unit: Count/s</p>	$\geq 0/s$	Shared load balancer	1 minute
m14_l7_rt	Average Layer-7 Response Time	<p>Average response time of the monitored object.</p> <p>This metric is available only when the frontend protocol is HTTP or HTTPS.</p> <p>The response time starts when the monitored object receives requests from the clients and ends when it returns all responses to the clients.</p> <p>Unit: ms</p> <p>NOTE The average response time it takes to establish a WebSocket connection may be very long. This metric cannot be used as a reference.</p>	≥ 0 ms	Shared load balancer	1 minute
m15_l7_upstream_4xx	4xx Status Codes Backend	<p>Number of 4xx status codes returned by the backend servers.</p> <p>This metric is available only when the frontend protocol is HTTP or HTTPS.</p> <p>Unit: Count/s</p>	$\geq 0/s$	Shared load balancer	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
m16_l7_upstream_5xx	5xx Status Codes Backend	<p>Number of 5xx status codes returned by the backend servers.</p> <p>This metric is available only when the frontend protocol is HTTP or HTTPS.</p> <p>Unit: Count/s</p>	$\geq 0/s$	Shared load balancer	1 minute
m17_l7_upstream_rt	Average Server Response Time	<p>Average response time of backend servers.</p> <p>The response time starts when the monitored object routes the requests to the backend server and ends when the monitored object receives a response from the backend server.</p> <p>This metric is available only when the frontend protocol is HTTP or HTTPS.</p> <p>Unit: ms</p> <p>NOTE The average response time it takes to establish a WebSocket connection may be very high. This metric cannot be used as a reference.</p>	≥ 0 ms	Shared load balancer	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
m1a_l7_upstream_rt_max	Maximum Server Response Time	<p>Maximum response time of backend servers.</p> <p>The response time starts when the monitored object routes the requests to the backend server and ends when the monitored object receives a response from the backend server.</p> <p>This metric is available only when the frontend protocol is HTTP or HTTPS.</p> <p>Unit: ms</p>	≥ 0 ms	Shared load balancer	1 minute
m1b_l7_upstream_rt_min	Minimum Server Response Time	<p>Minimum response time of backend servers.</p> <p>The response time starts when the monitored object routes the requests to the backend server and ends when the monitored object receives a response from the backend server.</p> <p>This metric is available only when the frontend protocol is HTTP or HTTPS.</p> <p>Unit: ms</p>	≥ 0 ms	Shared load balancer	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
m1c_l7_rt_max	Maximum Layer-7 Response Time	Maximum response time of the monitored object. The response time starts when the monitored object receives requests from the clients and ends when it returns all responses to the clients. This metric is available only when the frontend protocol is HTTP or HTTPS. Unit: ms	≥ 0 ms	Shared load balancer	1 minute
m1d_l7_rt_min	Minimum Layer-7 Response Time	Minimum response time of the monitored object. The response time starts when the monitored object receives requests from the clients and ends when it returns all responses to the clients. This metric is available only when the frontend protocol is HTTP or HTTPS. Unit: ms	≥ 0 ms	Shared load balancer	1 minute
m25_l7_resp_Bps	Backend Server Response Bandwidth	The bandwidth that the monitored object uses to return response to clients. Unit: bits/s NOTE When HTTP/2 is enabled for a listener, this metric cannot be used as a reference.	≥ 0 bit/s	Shared load balancer	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
m24_l7_req_Bps	Backend Server Request Bandwidth	The bandwidth that the monitored object uses to receive requests from clients. Unit: bits/s NOTE When HTTP/2 is enabled for a listener, this metric cannot be used as a reference.	≥ 0 bit/s	Shared load balancer	1 minute

Listener Metrics

Table 2-45 Metrics supported by each listener

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
m1_cps	Concurrent Connections	Load balancing at Layer 4: total number of TCP and UDP connections from the monitored object to backend servers. Load balancing at Layer 7: total number of TCP connections from the clients to the monitored object. Unit: Count	≥ 0	Shared load balancer - listener	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
m2_act_conn	Active Connections	<p>Number of TCP and UDP connections in the ESTABLISHED state between the monitored object and backend servers.</p> <p>You can run the following command to view the connections (both Windows and Linux servers): netstat -an</p> <p>Unit: Count</p>	≥ 0	Shared load balancer - listener	1 minute
m3_inact_conn	Inactive Connections	<p>Number of TCP connections between the monitored object and backend servers except those in the ESTABLISHED state.</p> <p>You can run the following command to view the connections (both Windows and Linux servers): netstat -an</p> <p>Unit: Count</p>	≥ 0	Shared load balancer - listener	1 minute
m4_ncps	New Connections	<p>Number of connections established between clients and the monitored object per second.</p> <p>Unit: Count/s</p>	≥ 0/s	Shared load balancer - listener	1 minute
m5_in_pps	Incoming Packets	<p>Number of packets received by the monitored object per second.</p> <p>Unit: Count/s</p>	≥ 0/s	Shared load balancer - listener	1 minute
m6_out_pps	Outgoing Packets	<p>Number of packets sent from the monitored object per second.</p> <p>Unit: Count/s</p>	≥ 0/s	Shared load balancer - listener	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
m7_in_Bps	Inbound Rate	Traffic used for accessing the monitored object from the Internet. Unit: bytes/s	≥ 0 byte/s	Shared load balancer - listener	1 minute
m8_out_Bps	Outbound Rate	Traffic used by the monitored object to access the Internet per second. Unit: bytes/s	≥ 0 byte/s	Shared load balancer - listener	1 minute
m22_in_bandwidth	Inbound Bandwidth	Bandwidth used for accessing the monitored object from the Internet. Unit: bits/s	≥ 0 bit/s	Shared load balancer - listener	1 minute
m23_out_bandwidth	Outbound Bandwidth	Bandwidth used by the monitored object to access the Internet. Unit: bits/s	≥ 0 bit/s	Shared load balancer - listener	1 minute
m1e_server_rps	Reset Packets from Backend Servers	Number of reset packets sent from backend servers to clients. These reset packets are generated by the backend servers and then forwarded by the load balancer. This metric is available only for TCP listeners. Unit: Count/s	≥ 0 /s	Shared load balancer - listener	1 minute
m21_client_rps	Reset Packets from Clients	Number of reset packets sent by clients to backend servers. These reset packets are generated by clients and then forwarded by the load balancer. This metric is available only for TCP listeners. Unit: Count/s	≥ 0 /s	Shared load balancer - listener	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
m1f_lvs_rps	Reset Packets from Load Balancers	Number of reset packets generated by the load balancer. This metric is available only for TCP listeners. Unit: Count/s	$\geq 0/s$	Shared load balancer - listener	1 minute
mb_l7_qps	Layer-7 Query Rate	Number of requests the monitored object receives per second. This metric is available only when the frontend protocol is HTTP or HTTPS. Unit: Count/s	$\geq 0/s$	Shared load balancer - listener	1 minute
mc_l7_http_2xx	Layer-7 2xx Status Codes	Number of 2xx status codes returned by the load balancer and backend servers. This metric is available only when the frontend protocol is HTTP or HTTPS. Unit: Count/s	$\geq 0/s$	Shared load balancer - listener	1 minute
md_l7_http_3xx	Layer-7 3xx Status Codes	Number of 3xx status codes returned by the load balancer and backend servers. This metric is available only when the frontend protocol is HTTP or HTTPS. Unit: Count/s	$\geq 0/s$	Shared load balancer - listener	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
me_l7_http_4xx	Layer-7 4xx Status Codes	Number of 4xx status codes returned by the load balancer and backend servers. This metric is available only when the frontend protocol is HTTP or HTTPS. Unit: Count/s	$\geq 0/s$	Shared load balancer - listener	1 minute
mf_l7_http_5xx	Layer-7 5xx Status Codes	Number of 5xx status codes returned by the load balancer and backend servers. This metric is available only when the frontend protocol is HTTP or HTTPS. Unit: Count/s	$\geq 0/s$	Shared load balancer - listener	1 minute
m10_l7_http_other_status	Layer-7 Other Status Codes	Number of status codes returned by the load balancer and backend servers except 2xx, 3xx, 4xx, and 5xx status codes. This metric is available only when the frontend protocol is HTTP or HTTPS. Unit: Count/s	$\geq 0/s$	Shared load balancer - listener	1 minute
m11_l7_http_404	Layer-7 404 Not Found	Number of 404 Not Found status codes returned by the load balancer and backend servers. This metric is available only when the frontend protocol is HTTP or HTTPS. Unit: Count/s	$\geq 0/s$	Shared load balancer - listener	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
m12_l7_http_499	Layer-7 499 Client Closed Request	<p>Number of 499 Client Closed Request status codes returned by the load balancer and backend servers.</p> <p>This metric is available only when the frontend protocol is HTTP or HTTPS.</p> <p>Unit: Count/s</p>	≥ 0/s	Shared load balancer - listener	1 minute
m13_l7_http_502	Layer-7 502 Bad Gateway	<p>Number of 502 Bad Gateway status codes returned by the load balancer and backend servers.</p> <p>This metric is available only when the frontend protocol is HTTP or HTTPS.</p> <p>Unit: Count/s</p>	≥ 0/s	Shared load balancer - listener	1 minute
m14_l7_rt	Average Layer-7 Response Time	<p>Average response time of the monitored object.</p> <p>This metric is available only when the frontend protocol is HTTP or HTTPS.</p> <p>The response time starts when the monitored object receives requests from the clients and ends when it returns all responses to the clients.</p> <p>Unit: ms</p> <p>NOTE The average response time it takes to establish a WebSocket connection may be very long. This metric cannot be used as a reference.</p>	≥ 0 ms	Shared load balancer - listener	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
m15_l7_upstream_4xx	4xx Status Codes Backend	<p>Number of 4xx status codes returned by the backend servers.</p> <p>This metric is available only when the frontend protocol is HTTP or HTTPS.</p> <p>Unit: Count/s</p>	≥ 0/s	Shared load balancer - listener	1 minute
m16_l7_upstream_5xx	5xx Status Codes Backend	<p>Number of 5xx status codes returned by the backend servers.</p> <p>This metric is available only when the frontend protocol is HTTP or HTTPS.</p> <p>Unit: Count/s</p>	≥ 0/s	Shared load balancer - listener	1 minute
m17_l7_upstream_rt	Average Server Response Time	<p>Average response time of backend servers.</p> <p>This metric is available only when the frontend protocol is HTTP or HTTPS.</p> <p>The response time starts when the monitored object routes the requests to the backend server and ends when the monitored object receives a response from the backend server.</p> <p>Unit: ms</p> <p>NOTE The average response time it takes to establish a WebSocket connection may be very long. This metric cannot be used as a reference.</p>	≥ 0 ms	Shared load balancer - listener	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
m1a_l7_upstream_rt_max	Maximum Server Response Time	<p>Maximum response time of backend servers.</p> <p>This metric is available only when the frontend protocol is HTTP or HTTPS.</p> <p>The response time starts when the monitored object routes the requests to the backend server and ends when the monitored object receives a response from the backend server.</p> <p>Unit: ms</p>	≥ 0 ms	Shared load balancer - listener	1 minute
m1b_l7_upstream_rt_min	Minimum Server Response Time	<p>Minimum response time of backend servers.</p> <p>This metric is available only when the frontend protocol is HTTP or HTTPS.</p> <p>The response time starts when the monitored object routes the requests to the backend server and ends when the monitored object receives a response from the backend server.</p> <p>Unit: ms</p>	≥ 0 ms	Shared load balancer - listener	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
m1c_l7_rt_max	Maximum Layer-7 Response Time	<p>Maximum response time of the monitored object.</p> <p>This metric is available only when the frontend protocol is HTTP or HTTPS.</p> <p>The response time starts when the monitored object receives requests from the clients and ends when it returns all responses to the clients.</p> <p>Unit: ms</p>	≥ 0 ms	Shared load balancer - listener	1 minute
m1d_l7_rt_min	Minimum Layer-7 Response Time	<p>Minimum response time of the monitored object.</p> <p>This metric is available only when the frontend protocol is HTTP or HTTPS.</p> <p>The response time starts when the monitored object receives requests from the clients and ends when it returns all responses to the clients.</p> <p>Unit: ms</p>	≥ 0 ms	Shared load balancer - listener	1 minute

Dimensions

Key	Value
lbaas_instance_id	ID of a shared load balancer
lbaas_listener_id	ID of a listener added to a shared load balancer

2.10.3 Viewing Traffic Usage

Scenarios

For livestreaming platforms, traffic often increases suddenly, which makes the services unstable. To address this issue, most of them use ELB to distribute traffic. By working with Cloud Eye, ELB allows you to monitor the traffic usage in real time. You can view the traffic consumed by the EIPs bound to public network load balancers to better balance your application workloads.

Prerequisites

Load balancers are running properly.

The associated backend servers are running normally and are not deleted or in the stopped or faulty state.

Viewing Traffic Usage of the Bound EIP



1. Log in to the management console.
2. In the upper left corner of the page, click  and select the desired region and project.
3. Click  in the upper left corner of the page and choose **Networking > Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Elastic IP and Bandwidth > EIPs**.
5. Locate the EIP bound to the load balancer and click its name. On the **Bandwidth** tab, you can view the data for the last 1, 3, 12 hours, last day, or last 7 days.

Figure 2-29 EIP traffic usage

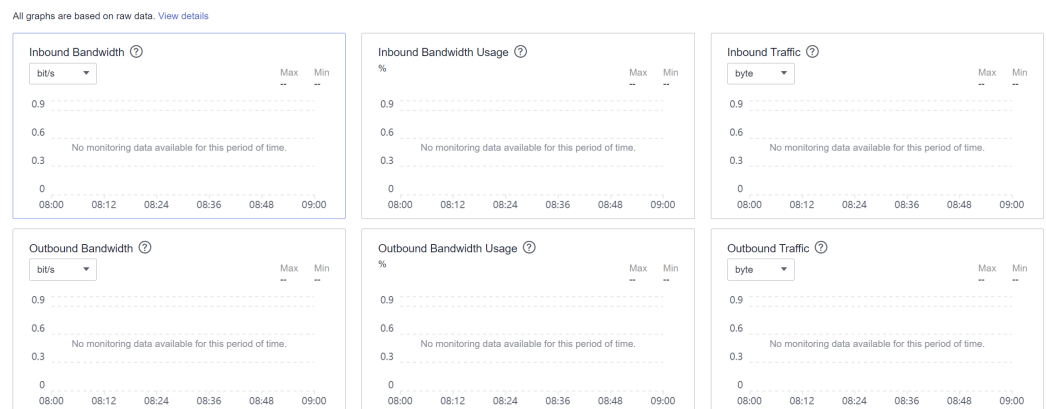


Table 2-46 EIP and bandwidth metrics

Metric	Meaning	Value Range	Monitored Object	Monitoring Period (Raw Data)
Outbound Bandwidth (originally named "Upstream Bandwidth")	Network rate of outbound traffic	≥ 0 bits/s	Bandwidth or EIP	1 minute
Inbound Bandwidth (originally named "Downstream Bandwidth")	Network rate of inbound traffic	≥ 0 bits/s	Bandwidth or EIP	1 minute
Outbound Bandwidth Usage	Usage of outbound bandwidth in percentage.	0-100%	Bandwidth or EIP	1 minute
Inbound Bandwidth Usage	Usage of inbound bandwidth in the unit of percent.	0-100%	Bandwidth or EIP	1 minute
Outbound Traffic (originally named "Upstream Traffic")	Network traffic going out of the cloud platform	≥ 0 bytes	Bandwidth or EIP	1 minute
Inbound Traffic (originally named "Downstream Traffic")	Network traffic going into the cloud platform	≥ 0 bytes	Bandwidth or EIP	1 minute

Viewing Load Balancer Traffic Metrics

1. Go to the [load balancer list page](#).
2. On the load balancer list page, locate the load balancer and click its name.
3. Click the **Monitoring** tab, select load balancer for **Dimension**, and view the graphs of inbound and outbound rates.

You can view data from the last 1, 3, 12 hours, last day, or the last 7 days.

2.11 Auditing

2.11.1 Key Operations Recorded by CTS

You can use CTS to record operations on ELB for query, auditing, and backtracking.

[Table 2-47](#) lists the operations recorded by CTS.

Table 2-47 ELB operations recorded by CTS

Action	Resource Type	Trace Name
Configuring access logs	logtank	createLogtank
Deleting access logs	logtank	deleteLogtank
Creating a certificate	certificate	createCertificate
Modifying a certificate	certificate	updateCertificate
Deleting a certificate	certificate	deleteCertificate
Creating a health check	healthmonitor	createHealthMonitor
Modifying a health check	healthmonitor	updateHealthMonitor
Deleting a health check	healthmonitor	deleteHealthMonitor
Adding a forwarding policy	l7policy	createL7policy
Modifying a forwarding policy	l7policy	updateL7policy
Deleting a forwarding policy	l7policy	deleteL7policy
Adding a forwarding rule	l7rule	createL7rule
Modifying a forwarding rule	l7rule	updateL7rule
Deleting a forwarding rule	l7rule	deleteL7rule


Action	Resource Type	Trace Name
Adding a listener	listener	createListener
Modifying a listener	listener	updateListener
Deleting a listener	listener	deleteListener
Creating a load balancer	loadbalancer	createLoadbalancer
Modifying a load balancer	loadbalancer	updateLoadbalancer
Deleting a load balancer	loadbalancer	deleteLoadbalancer
Adding a backend server	member	createMember
Modifying a backend server	member	updateMember
Removing a backend server	member	batchUpdateMember
Creating a backend server group	pool	createPool
Modifying a backend server group	pool	updatePool
Deleting a backend server group	pool	deletePool

2.11.2 Viewing Traces

Scenarios

CTS records the operations performed on ELB and allows you to view the traces of the last seven days on the CTS console. To query these traces, perform the following operations.

Procedure

1. Log in to the management console.
2. In the upper left corner of the page, click  and select the desired region and project.
3. Under **Management & Governance**, click **Cloud Trace Service**.
4. In the navigation pane on the left, choose **Trace List**.
5. Specify the filters used for querying traces. The following filters are available:


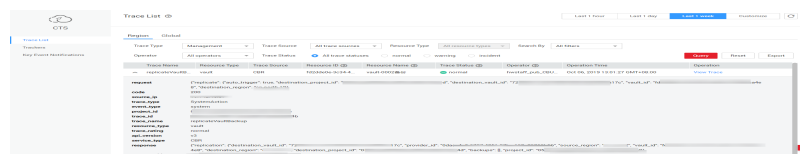
- **Trace Type, Trace Source, Resource Type, and Search By**
Select a filter from the drop-down list.
If you select **Trace name** for **Search By**, you need to select a specific trace name.
If you select **Resource ID** for **Search By**, select or enter a specific resource ID.
If you select **Resource name** for **Search By**, select or enter a specific resource name.
 - **Operator:** Select a specific operator (at the user level rather than the tenant level).
 - **Trace Status:** Available options include **All trace statuses, Normal, Warning, and Incident**. You can only select one of them.
 - **Time range:** You can query traces generated at any time range of the last seven days.
6. Click  on the left of the required trace to expand its details.

Figure 2-30 Expanding trace details



7. Click **View Trace** in the **Operation** column to view trace details.

Figure 2-31 View Trace

```

"context": {
  "code": "204",
  "source_ip": "10.45.152.59",
  "trace_type": "ApiCall",
  "event_type": "system",
  "project_id": "0503dda897000fed2f78c00909158a4d",
  "trace_id": "116a2aff-deb8-11e9-95f5-d5c0b02a9b97",
  "trace_name": "deleteMember",
  "resource_type": "member",
  "trace_rating": "normal",
  "api_version": "v2.0",
  "service_type": "ELB",
  "response": "{\"member\": {\"project_id\": \"0503dda897000fed2f78c00909158a4d\", \"name\": \"9646e73b-338c-4d27-a17c-219be532812c\", \"resource_id\": \"9646e73b-338c-4d27-a17c-219be532812c\"}}, \"code\": 204, \"message\": \"OK\"}",
  "tracker_name": "system",
  "time": "1569321775225",
  "resource_name": "9646e73b-338c-4d27-a17c-219be532812c",
  "record_time": "1569321775903",
  "user": {
    "domain": {
      "name": "huaweicloud.com",
      "id": "0503dda878000fed0f75c0096d70a960"
    }
  }
},

```

For details about key fields in the trace, see the [Cloud Trace Service User Guide](#).

Example Traces

- **Creating a load balancer**
request {"loadbalancer":{"name":"elb-test-zcy","description":"","tenant_id":"05041ffa40025702f6dc009cc6f8f33","vip_subnet_id":"ed04fd93-e74b-4794-b63e-e72baa02a2da","admin_state_up":true}}
code 201
source_ip 124.71.93.36
trace_type ConsoleAction

```
event_type system
project_id 05041fffa40025702f6dc009cc6f8f33
trace_id b39b21a1-8d49-11ec-b548-2be046112888
trace_name createLoadbalancer
resource_type loadbalancer
trace_rating normal
api_version v2.0
service_type ELB
response {"loadbalancer": {"description": "", "provisioning_status": "ACTIVE", "provider": "vlb",
"project_id": "05041fffa40025702f6dc009cc6f8f33", "vip_address": "172.18.0.205", "pools": [],
"operating_status": "ONLINE", "name": "elb-test-zcy", "created_at": "2022-02-14T03:53:39",
"listeners": [], "id": "7ebe23cd-1d46-4a49-b707-1441c7f0d0d1", "vip_port_id":
"5b36ff96-3773-4736-83cf-38c54abedeea", "updated_at": "2022-02-14T03:53:41", "tags": [],
"admin_state_up": true, "vip_subnet_id": "ed04fd93-e74b-4794-b63e-e72baa02a2da", "tenant_id":
"05041fffa40025702f6dc009cc6f8f33"}}
resource_id 7ebe23cd-1d46-4a49-b707-1441c7f0d0d1
tracker_name system
time 2022/02/14 11:53:42 GMT+08:00
resource_name elb-test-zcy
record_time 2022/02/14 11:53:42 GMT+08:00
request_id
user {"domain": {"name": "CBUInfo", "id": "0503dda87802345ddafed096d70a960"}, "name": "zcy",
"id": "09f106afd2345cdeff5c009c58f5b4a"}
```

- **Deleting a load balancer**

```
request
code 204
source_ip 124.71.93.36
trace_type ConsoleAction
event_type system
project_id 05041fffa40025702f6dc009cc6f8f33
trace_id 4f838bbf-8d4a-11ec-a1fe-1f93fdaf3bec
trace_name deleteLoadbalancer
resource_type loadbalancer
trace_rating normal
api_version v2.0
service_type ELB
response {"loadbalancer": {"listeners": [], "vip_port_id": "5b36ff96-3773-4736-83cf-38c54abedeea",
"tags": [], "tenant_id": "05041fffa40025702f6dc009cc6f8f33", "admin_state_up": true, "id":
"7ebe23cd-1d46-4a49-b707-1441c7f0d0d1", "operating_status": "ONLINE", "description": "", "pools":
[], "vip_subnet_id": "ed04fd93-e74b-4794-b63e-e72baa02a2da", "project_id":
"05041fffa40025702f6dc009cc6f8f33", "provisioning_status": "ACTIVE", "name": "elb-test-zcy",
"created_at": "2022-02-14T03:53:39", "vip_address": "172.18.0.205", "updated_at":
"2022-02-14T03:53:41", "provider": "vlb"}}
resource_id 7ebe23cd-1d46-4a49-b707-1441c7f0d0d1
tracker_name system
time 2022/02/14 11:58:03 GMT+08:00
resource_name elb-test-zcy
record_time 2022/02/14 11:58:03 GMT+08:00
request_id
user {"domain": {"name": "CBUInfo", "id": "0503dda87802345ddafed096d70a960"}, "name": "zcy", "id":
"09f106afd2345cdeff5c009c58f5b4a"}
```

3 Self-service Troubleshooting

3.1 Overview

ELB self-service troubleshooting helps you detect and fix unhealthy backend servers in a timely manner. It also gets you familiar with billing and service features that you might be curious about. During the troubleshooting process, resource configurations will not be changed and services will work normally.

You may find the answers to the issues listed in [Table 3-1](#).

Table 3-1 ELB self-service troubleshooting

Issue	Description
Troubleshooting an Unhealthy Backend Server	<ul style="list-style-type: none">• Checks the security group rules.• Checks the network ACL configurations.• Checks the health check ports.
ELB Billing	Describes how ELB is billed.
Differences Between Dedicated and Shared Load Balancers	Describes the advantages of each type of load balancer.

3.2 Troubleshooting an Unhealthy Backend Server

Scenarios

This section describes how you can use ELB self-service troubleshooting to detect and fix unhealthy backend servers in a timely manner.

Prerequisites



Before troubleshooting an unhealthy backend server, make sure you have completed the following:

- [Creating a Backend Server Group](#)
- [Adding a TCP Listener](#)
- [Configuring a Health Check](#)

Notes and Constraints

- You can only troubleshoot an unhealthy backend server.
- The backend server must be associated with a listener.
- IP as backend servers does not support self-service troubleshooting.

Procedure

1. Log in to the management console.
2. In the upper left corner of the page, click  and select the desired region and project.
3. Click  in the upper left corner to display **Service List** and choose **Networking > Elastic Load Balance**.
4. In the navigation pane on the left, click **Self-service Troubleshooting**.
5. On the **Elastic Load Balance** tab, click **Unhealthy backend servers**.
6. Select the load balancer that has unhealthy backend servers.
7. Select the unhealthy backend server you want to troubleshoot.
8. Click **Troubleshoot**. On the displayed page, view the troubleshooting progress and details.

View and rectify the faults in a timely manner as described in [Table 3-2](#).

Table 3-2 Health check items

Health Check Category	Health Check Item	Reason	Suggestion
Security group rule configurations	The protocol configured for the inbound rule	The inbound rules of the security group do not allow traffic over the health check protocol.	Change the security group rules by referring to the following: <ul style="list-style-type: none"> • Security Group and Network ACL Rules • Security Group and Network ACL Rules
	The source configured for the inbound rule	The inbound rules of the security group do not allow traffic from the health check IP address to the backend server.	

Health Check Category	Health Check Item	Reason	Suggestion
	The port configured for the inbound rule	The inbound rules of the security group do not allow traffic over the health check port.	
	The protocol configured for the outbound rule	The outbound rules of the security group do not allow traffic over the health check protocol.	
	The destination configured for the outbound rule	The outbound rules of the security group do not allow traffic from the backend server to the health check IP address.	
	The port configured for the outbound rule	The outbound rules of the security group do not allow traffic over the health check port.	
Network ACL rule configurations	The protocol configured for the inbound rule	The inbound rules of the network ACL do not allow traffic over the health check protocol.	Change the network ACL rules by referring to the following: <ul style="list-style-type: none"> ● Security Group and Network ACL Rules ● Security Group and Network ACL Rules
	The source configured for the inbound rule	The inbound rules of the network ACL do not allow traffic from the health check IP address to the backend server.	
	The source port configured for the inbound rule	The inbound rules of the network ACL do not allow traffic over all source ports.	

Health Check Category	Health Check Item	Reason	Suggestion
	The destination address configured for the inbound rule	The inbound rules of the network ACL do not allow traffic to the destination address.	
	The destination port configured for the inbound rule	The inbound rules of the network ACL do not allow traffic over the destination port.	
	The protocol configured for the outbound rule	The outbound rules of the network ACL do not allow traffic over the health check protocol.	
	The destination configured for the outbound rule	The outbound rules of the network ACL do not allow traffic from the health check IP address to the backend server.	
	The source port configured for the outbound rule	The outbound rules of the network ACL do not allow traffic over the health check port.	
	The destination address configured for the outbound rule	The outbound rules of the network ACL do not allow traffic to the destination address.	

Health Check Category	Health Check Item	Reason	Suggestion
	The destination port configured for the outbound rule	The outbound rules of the network ACL do not allow traffic over all destination ports.	
Health check configurations	The port configured for the health check	The specified health check port is different from that used by the backend server.	Use the backend port as the health check port by referring to Configuring a Health Check .

 **NOTE**

- If all the check items are reported as normal, perform further checks as guided by [How Do I Troubleshoot an Unhealthy Backend Server?](#)
- If the troubleshooting fails, click **Troubleshoot Again** or perform further checks as guided by [How Do I Troubleshoot an Unhealthy Backend Server?](#)

3.3 Other Issues

You can also use ELB self-service troubleshooting to find the answers to the following issues:

- [ELB Billing](#)
- [Differences Between Dedicated and Shared Load Balancers](#)

ELB Billing

You can learn more about ELB billing as described in [Table 3-3](#).

Table 3-3 ELB billing

Scenario	Reference
Billing rules	<ul style="list-style-type: none"> • Billing Items (Dedicated Load Balancers) • Billing Items (Shared Load Balancers)
Specifications	Modifying Specifications

Differences Between Dedicated and Shared Load Balancers

Learn more about the advantages of each type of load balancer as described in [Table 3-4](#).

Table 3-4 Differences

Scenario	Reference
Feature comparison	Differences Between Dedicated and Shared Load Balancers
Creating a backend server group	<ul style="list-style-type: none">• Creating a Backend Server Group• Creating a Backend Server Group
Adding a backend server	<ul style="list-style-type: none">• Backend Server Overview• Backend Server Overview

4 Appendix

4.1 Configuring the TOA Module

Scenarios

ELB provides customized strategies for managing service access. Before these strategies can be customized, the clients' IP addresses contained in the requests are required. To obtain the IP addresses, you can install the TCP Option Address (TOA) kernel module on backend servers.

This section provides detailed operations for you to compile the module in the OS if you use TCP to distribute incoming traffic.

The operations for Linux OSs with kernel version of 2.6.32 are different from those for Linux OSs with kernel version of 3.0 or later.

NOTE

- TOA does not support listeners using the UDP protocol.
- The module can work properly in the following OSs and the methods for installing other kernel versions are similar:
 - CentOS 6.8 (kernel version 2.6.32)
 - SUSE 11 SP3 (kernel version 3.0.76)
 - CentOS 7 and CentOS 7.2 (kernel version 3.10.0)
 - Ubuntu 16.04.3 (kernel version 4.4.0)
 - Ubuntu 18.04 (kernel version 4.15.0)
 - Ubuntu 20.04 (Kernel version 5.4.0)
 - OpenSUSE 42.2 (kernel version 4.4.36)
 - Debian 8.2.0 (kernel version 3.16.0)

Prerequisites

- The development environment for compiling the module must be the same as that of the current kernel. For example, if the kernel version is kernel-3.10.0-693.11.1.el7, the kernel development package version must be kernel-devel-3.10.0-693.11.1.el7.

- Servers can access OS repositories.
- Users other than **root** must have sudo permissions.

Procedure

- In the following operations, the Linux kernel version is 3.0 or later.
1. Prepare the compilation environment.

NOTE

- During the installation, download the required module development package from the Internet if it cannot be found in the source.
- If the kernel development package (kernel-devel) cannot be obtained, contact the image provider.

The following are operations for compiling the module in different Linux OSs. Perform appropriate operations.

– CentOS

- i. Run the following command to install the GCC:

```
sudo yum install gcc
```

- ii. Run the following command to install the make tool:

```
sudo yum install make
```

- iii. Run the following command to install the module development package (the package header and module library must have the same version as the kernel):

```
sudo yum install kernel-devel-`uname -r`
```

NOTE

- During the installation, download the required module development package from the following address if it cannot be found in the source:
https://mirror.netcologne.de/oracle-linux-repos/ol7_latest/getPackage/
For example, to install 3.10.0-693.11.1.el7.x86_64, run the following command:

```
rpm -ivh kernel-devel-3.10.0-693.11.1.el7.x86_64.rpm
```
- If the kernel development package (kernel-devel) cannot be obtained, contact the image provider.

– Ubuntu and Debian

- i. Run the following command to install the GCC:

```
sudo apt-get install gcc
```

- ii. Run the following command to install the make tool:

```
sudo apt-get install make
```


- iii. Run the following command to install the module development package (the package header and module library must have the same version as the kernel):

```
sudo apt-get install linux-headers-`uname -r`
```

– SUSE


- i. Run the following command to install the GCC:

```
sudo zypper install gcc
```


- ii. Run the following command to install the make tool:
sudo zypper install make
 - iii. Run the following command to install the module development package (the package header and module library must have the same version as the kernel):
sudo zypper install kernel-default-devel
2. Compile the module.
 - a. Use the git tool and run the following command to download the module source code:
git clone https://github.com/Huawei/TCP_option_address.git
 **NOTE**

If the git tool is not installed, download the module source code from the following link:
https://github.com/Huawei/TCP_option_address
 - b. Run the following commands to enter the source code directory and compile the module:
cd src
make

If no warning or error code is prompted, the compilation was successful. Verify that the **toa.ko** file was generated in the current directory.

 **NOTE**
 - If error message "config_retpoline=y but not supported by the compiler, Compiler update recommended" is displayed, the GCC version is outdated. Upgrade the GCC to a later version.
 - If the kernel version has been manually upgraded in the standard Linux distribution and the TOA module fails to be compiled, you are advised to upgrade the GCC to a later version.
3. Load the module.
 - a. Run the following command to load the module:
sudo insmod toa.ko
 - b. Run the following command to check the module loading and to view the kernel output information:
dmesg | grep TOA

If **TOA: toa loaded** is displayed in the command output, the module has been loaded.

 **NOTE**

After compiling the CoreOS module in the container, copy it to the host system and then load it. The container for compiling the module shares the **/lib/modules** directory with the host system, so you can copy the module in the container to this directory, allowing the host system to use it.
4. Set the script to enable it to automatically load the module.

To make the module take effect when the system starts, add the command for loading the module to your startup script.

You can use either of the following methods to automatically load the module:

- Add the command for loading the module to a customized startup script as required.
- Perform the following operations to configure a startup script:

- i. Create the **toa.modules** file in the **/etc/sysconfig/modules/** directory. This file contains the module loading script.

The following is an example of the content in the **toa.modules** file.

```
#!/bin/sh
/sbin/modinfo -F filename /root/toa/toa.ko > /dev/null 2>&1
if [ $? -eq 0 ]; then
/sbin/insmod /root/toa/toa.ko
fi
```

/root/toa/toa.ko is the path of the module file. You need to replace it with their actual path.

- ii. Run the following command to add execution permissions for the **toa.modules** startup script:

```
sudo chmod +x /etc/sysconfig/modules/toa.modules
```

NOTE

If the kernel is upgraded, the current module will no longer match. Compile the module again.

5. Install the module on multiple servers.

To load the module in the same OS, copy the **toa.ko** file to servers where the module is to be loaded and then perform the operations in [3](#).

After the module is successfully loaded, applications can obtain the real IP address contained in the request.

NOTE

The OS of the server must have the same version as the kernel.

6. Verify the module.

After the module is successfully installed, the source address can be directly obtained. The following provides an example for verification.

Run the following command to start SimpleHTTPServer on the backend server where Python is installed:

```
python -m SimpleHTTPServer port
```

The value of **port** must be the same as the port configured for the backend server, and the default value is **80**.

Access the IP address of the load balancer from a client. Access logs on the server are as follows:

```
192.168.0.90 -- [06/Aug/2020 14:24:21] "GET / HTTP/1.1" 200 -
```

NOTE

192.168.0.90 indicates the client's source IP address that is obtained by the backend server.

- In the following operations, the Linux kernel version is 2.6.32.

NOTE

The TOA plug-in supports the OSs (CentOS 6.8 image) with a kernel of 2.6.32-xx. Perform the following steps to configure the module:

1. Obtain the kernel source code package
Linux-2.6.32-220.23.1.el6.x86_64.rs.src.tar.gz containing the module from the following link:
http://kb.linuxvirtualserver.org/images/3/34/Linux-2.6.32-220.23.1.el6.x86_64.rs.src.tar.gz
2. Decompress the kernel source code package.
3. Modify compilation parameters.
 - a. Open the **linux-2.6.32-220.23.1.el6.x86_64.rs** folder.
 - b. Edit the **net/toa/toa.h** file.
Change the value of **#define TCPOPT_TOA200** to **#define TCPOPT_TOA254**.
 - c. On the shell page, run the following commands:
sed -i 's/CONFIG_IPV6=m/CONFIG_IPV6=y/g' .config
echo -e '\n# toa\nCONFIG_TOA=m' >> .config
After the configuration, the IPv6 module is compiled into the kernel. TOA is compiled into a separate module and can be independently started and stopped.
 - d. Edit **Makefile**.
You can add a description to the end of **EXTRAVERSION =**. This description will be displayed in **uname -r**, for example, **-toa**.
4. Run the following command to compile the software package:
make -j n

NOTE

n indicates the number of vCPUs. For example, if there are four vCPUs, *n* must be set to 4.

5. Run the following command to install the module:
make modules_install

The following information is displayed.

Figure 4-1 Installing the module

```
INSTALL /lib/firmware/kaweth/trigger_code_fix.bin
INSTALL /lib/firmware/ti_3410.fw
INSTALL /lib/firmware/ti_5052.fw
INSTALL /lib/firmware/mts_cdma.fw
INSTALL /lib/firmware/mts_gsm.fw
INSTALL /lib/firmware/mts_edge.fw
INSTALL /lib/firmware/edgeport/boot.fw
INSTALL /lib/firmware/edgeport/boot2.fw
INSTALL /lib/firmware/edgeport/down.fw
INSTALL /lib/firmware/edgeport/down2.fw
INSTALL /lib/firmware/edgeport/down3.bin
INSTALL /lib/firmware/whiteheat_loader.fw
INSTALL /lib/firmware/whiteheat.fw
INSTALL /lib/firmware/keyspan_pda/keyspan_pda.fw
INSTALL /lib/firmware/keyspan_pda/xircom_pgs.fw
DEPMOD 2.6.32-toa
```

6. Run the following command to install the kernel:

make install

The following information is displayed.

Figure 4-2 Installing the kernel

```
INSTALL /lib/firmware/keyspan_pda/xircom_pgs.fw
DEPMOD 2.6.32-toa
[root@SZX1000167219 linux-2.6.32-220.23.1.el6.x86_64.rs]# make install
sh /root/humin/linux-2.6.32-220.23.1.el6.x86_64.rs/arch/x86/boot/install.sh 2.6.32-toa arch/x86/boot/bzImage \
System.map "/boot"
ERROR: modinfo: could not find module xen_procfs
ERROR: modinfo: could not find module ipv6
ERROR: modinfo: could not find module xen_scscifront
ERROR: modinfo: could not find module xen_hcall
ERROR: modinfo: could not find module xen_balloon
[root@SZX1000167219 linux-2.6.32-220.23.1.el6.x86_64.rs]#
```

7. Open the **/boot/grub/grub.conf** file and configure the kernel to start up when the system starts.
 - a. Change the default startup kernel from the first kernel to the zeroth kernel by changing **default=1** to **default=0**.
 - b. Add the **nohz=off** parameter to the end of the line containing the **vmlinuz-2.6.32-toa** kernel. If **nohz** is not disabled, the CPU0 utilization may be high and overload the kernel.

Figure 4-3 Configuration file

```
default=1
timeout=5
splashimage=(hd0,1)/boot/grub/splash.xpm.gz
hiddenmenu
title Red Hat Enterprise Linux Server (2.6.32-toa)
    root (hd0,1)
    kernel /boot/vmlinuz-2.6.32-toa ro root=UUID=
et nohz=off
    initrd /boot/initramfs-2.6.32-toa.img
```

- c. Save the modification and exit. Restart the OS.
During the restart, the system will load the **vmlinuz-2.6.32-toa** kernel.
8. After the restart, run the following command to load the module:

modprobe toa

Add the **modprobe toa** command to both the startup script and the system scheduled monitoring script.

Figure 4-4 Adding the **modprobe toa** command

```
[root@SZX1000167219 ~]# modprobe toa
[root@SZX1000167219 ~]# lsmod |grep toa
toa                4203  0
[root@SZX1000167219 ~]#
```

After the module is loaded, query the kernel information.

Figure 4-5 Querying the kernel

```
[root@SZX1000167219 ~]# uname -a
Linux SZX1000167219 2.6.32-toa #1 SMP Sat Oct 15 11:50:05 CST 2016 x86_64 x86_64 x86_64 GNU/Linux
```


9. Verify the module.

After the module is installed, the source IP address can be directly obtained. The following provides an example for verification.

Run the following command to start SimpleHTTPServer on the backend server where Python is installed:

```
python -m SimpleHTTPServer port
```

The value of **port** must be the same as the port configured for the backend server, and the default value is **80**.

Access the IP address of the load balancer from a client. Access logs on the server are as follows:

```
192.168.0.90 - - [06/Aug/2020 14:24:21] "GET / HTTP/1.1" 200 -
```

 **NOTE**

192.168.0.90 indicates the client's source IP address that is obtained by the backend server.