Alibaba Cloud Server Load Balancer

Listeners

Issue: 20190816

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. **You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.**
2. **No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.**
3. **The content of this document may be changed due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.**
4. **This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity , applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use**

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd /d C:/windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	**It indicates that it is a required value, and only one item can be selected.**	`swich {stand | slave}`

Contents

1 Listener overview

After you create a Server Load Balancer (SLB) instance, you must configure a listener for it. The listener checks connection requests and then distributes the requests to backend servers according to configured forwarding rules.

Alibaba Cloud provides Layer-4 (TCP and UDP protocols) and Layer-7 (HTTP and HTTPS protocols) load balancing services. Select the protocol based on your needs.

Protocol	Description	Scenario
TCP	· A connection-oriented protocol. A reliable connection must be established before data can be sent and received. · Source IP address-based session persistence. · Source IP addresses can be read at the network layer. · Fast data transmission.	· Applicable to scenarios where high transmission reliability and data accuracy are required, but some flexibility regarding network latency is permitted, such as file transmission, sending or receiving emails, and remote logons. · Web applications that have no special requirements. For more information, see Add a TCP listener.
UDP	· A non-connection-oriented protocol. UDP directly transmits data packets instead of making a three-way handshake with the other party before sending data. It does not provide error recovery and data re-transmission. · Fast data transmission, but the reliability is relatively low.	Applicable to scenarios with preference to real-time content over reliability, such as video chats and real-time financial quotations. For more information, see #unique_5.

Protocol	Description	Scenario
HTTP	· An application layer protocol mainly used to package data. · Cookie-based session persistence. · Use X-Forward-For to obtain source IP addresses.	Applicable to applications that need to recognize data content , such as web applications and small-sized mobile games. For more information, see #unique_6.
HTTPS	· Encrypted data transmission that prevents unauthorized access. · Unified certificate management service. You can upload certificates to SLB and decryption operations are completed directly on SLB.	Applications that require encrypted transmission. For more information, see #unique_7.

Note:
HTTP/2 and WSS/WS protocols are supported by all regions now. For more information, see HTTP/2 support FAQ and #unique_8.

2 Add a TCP listener

This topic describes how to add a TCP listener to a Server Load Balancer (SLB) instance. The TCP protocol is applicable to scenarios with high requirements on reliability and data accuracy but with tolerance for low speed, such as file transmission, sending or receiving emails, and remote logons. You can add a TCP listener to forward requests from the TCP protocol.

Prerequisites

An SLB instance is created. For more information, see #unique_10.

Step 1 Open the listener configuration wizard

To open the listener configuration wizard, follow these steps:

1. Log on to the Server Load Balancer console.
2. In the left-side navigation pane, choose Instances > Server Load Balancer.
3. Select the region of the target SLB instance.
4. Select one of the following methods to open the listener configuration wizard:
   - On the Server Load Balancer page, find the target SLB instance and then click Configure Listener in the Actions column.
   - On the Server Load Balancer page, click the ID of the target SLB instance. On the Listeners tab, click Add Listener.

Step 2 Configure the TCP listener

To configure the TCP listener, follow these steps:

1. Configure the TCP listener according to the following information:

Configuration	Description
Select Listener Protocol	Select the protocol type of the listener. In this topic, select TCP.

Configuration	Description
Listening Port	The listening port used to receive requests and forward the requests to backend servers. The port number is in the range of 1 to 65535. Note: In the same SLB instance, the UDP or TCP listener port numbers can be the same in the following regions. However, you must first apply for the privilege to use the beta function of configuring the same ports in TCP/UDP listeners on the Quota Management page of the SLB console. In other cases, the listener port numbers must be unique. · UAE (Dubai) · Australia (Sydney) · UAE (Dubai) · UK (London) · Germany (Frankfurt) · US (Silicon Valley) · US (Virginia) · Indonesia (Jakarta) · Japan (Tokyo) · India (Mumbai) · Singapore · Malaysia (Kuala Lumpur) · China (Hong Kong) · China (Shenzhen) · China (Hohhot) · China (Qingdao) · China (Chengdu) · China (Zhangjiakou) · China (Shanghai)
Advanced configurations	

Configuration	Description
Scheduling Algorithm	SLB supports four scheduling algorithms: round robin, weighted round robin (WRR), weighted least connections (WLC), and consistent hash. · Weighted Round-Robin (WRR): A backend server with a higher weight receives more requests. · Round-Robin (RR): Requests are evenly and sequentially distributed to backend servers. · Weighted Least Connections (WLC): A server with a higher weight receives more requests. When the weight values of two backend servers are the same, the backend server with a smaller number of connections is more likely to be polled. · Consistent Hash (CH): - Source IP: the consistent hash based on source IP addresses. Requests from the same source IP address are scheduled to the same backend server. - Tuple: the consistent hash based on four factors: source IP address + destination IP address + source port + destination port. The same streams are scheduled to the same backend server. Note: Currently, the Consistent Hash (CH) algorithm is only supported in the following regions: - Japan (Tokyo) - Australia (Sydney) - Malaysia (Kuala Lumpur) - Indonesia (Jakarta) - Germany (Frankfurt) - US (Silicon Valley) - US (Virginia) - UAE (Dubai) - China (Hohhot) - UK (London) - Zone B and Zone C of Singapore - China (Hong Kong) - China (Qingdao) - China (Zhangjiakou)

Configuration	Description
Enable Session Persistence	Select whether to enable session persistence. If you enable session persistence, all session requests from the same client are sent to the same backend server. For TCP listeners, session persistence is based on IP addresses. Requests from the same IP address are forwarded to the same backend server.
Enable Access Control	Select whether to enable the access control function.
Access Control Method	Select an access control method after you enable the access control function: · Whitelist: Only requests from IP addresses or CIDR blocks in the selected access control list are forwarded. It applies to scenarios where the application only allows access from some specific IP addresses. Enabling a whitelist poses some risks to your services. After a whitelist is configured, only the IP addresses in the list can access the SLB listener . If you enable the whitelist without adding any IP addresses in the corresponding access control list, all requests are forwarded. · Blacklist: Requests from IP addresses or CIDR blocks in the selected access control list are not forwarded. It applies to scenarios where the application only denies access from some specific IP addresses. If you enable a blacklist without adding any IP addresses in the corresponding access control list, all requests are forwarded.

Configuration	Description
Access Control List	Select an access control list as the whitelist or the blacklist.  Note: An IPv6 instance can only be associated with IPv6 access control lists and an IPv4 instance can only be associated with IPv4 access control lists. For more information, see Configure an access control list.
Enable Peak Bandwidth Limit	Select whether to configure the listening bandwidth. If the SLB instance is charged based on bandwidth , you can set different peak bandwidth values for different listeners to limit the traffic passing through each listener. The sum of the peak bandwidth values of all listeners under an SLB instance cannot exceed the bandwidth value of that SLB instance. By default, all listeners share the bandwidth of the SLB instance.  Note: SLB instances billed by traffic have no peak bandwidth limit by default.
Idle Timeout	Specify the idle connection timeout period. Value range: 10 to 900. Unit: seconds.
Listener Name	Enter a name for the TCP listener to be added.
Get Client Source IP Address	Backend servers of a Layer-4 listener can directly obtain the source IP addresses of clients.
Automatically Enable Listener after Creation	Choose whether to start the listener after the listener is configured. The listener is started by default.

2. Click Next.

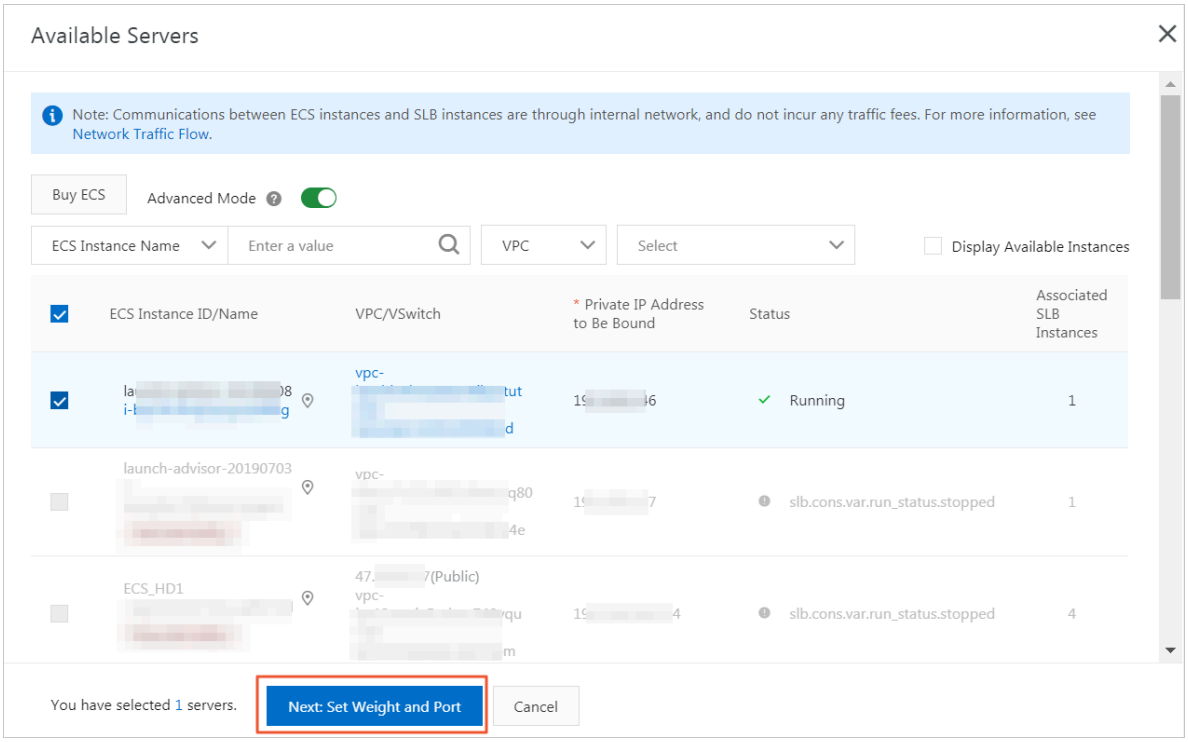
Step 3 Add backend servers

After configuring the listener, you need to add backend servers to process requests. You can use the default server group configured for the SLB instance, or configure a VServer group or an active/standby server group for the listener. For more information, see #unique_12.

In this example, use the default server group.

1. Select Default Server Group and then click Add More.

2. Select the ECS instances to add, and then click Next: Set Weight and Port.



3. Configure ports and weights for the added backend servers (ECS instances).

   - Port

     The port opened on the backend server to receive requests. The port number is in the range of 1 to 65535. Ports of backend servers can be the same in an SLB instance.

   - Weight

     The weight of the backend server. A backend server with a higher weight receives more requests.

     Note:
     If the weight is set to 0, no requests are sent to the backend server.

4. Click Next.

Step 4 Configure health checks

SLB checks the service availability of backend servers by performing health checks. The health check function improves the overall availability of your services and avoids the impact of backend server failures. Click Modify to change health check configurations. For more information, see #unique_13.

Step 5 Submit the configurations

To submit the listener configurations, follow these steps:

1. On the Submit page, check the listener configurations. You can click Modify to change the configurations.
2. Click Submit.
3. On the Submit page, click OK after the configurations are successful.

   After the configurations are successful, you can view the created listener on the Listeners page.

#unique_14

#unique_15

#unique_16

#unique_17

#unique_18

3 Add a UDP listener

This topic describes how to add a UDP listener to a Server Load Balancer (SLB) instance. You can add a UDP listener to forward requests from the UDP protocol.

Prerequisites

An SLB instance is created. For more information, see #unique_10.

Context

Note the following before you add a UDP listener:

- Currently, ports 250, 4789, and 4790 are reserved.
- Currently, fragmented packets are not supported.
- UDP listeners of an SLB instance of the classic network do not support viewing source IP addresses.
- The following operations require five minutes to take effect if they are performed in a UDP listener:
  - Remove a backend ECS instance.
  - Set the weight of a backend server to 0 after the backend server is declared as unhealthy.
- Because IPv6 has a longer IP header than IPv4, when you use a UDP listener on an IPv6 SLB instance, you must ensure that the MTU of the NIC on the backend server (ECS instance) communicating with the SLB instance is not greater than 1480 (some applications need to synchronize its configuration files based on this MTU value). Otherwise, packets may be discarded because they are too large.

  If you use a TCP, HTTP, or HTTPS listener, no additional configurations are required because the TCP protocol supports MSS auto-negotiation.

Step 1 Open the listener configuration wizard

To open the listener configuration wizard, follow these steps:

1. Log on to the Server Load Balancer console.
2. In the left-side navigation pane, choose Instances > Server Load Balancer.
3. Select the region of the target SLB instance.

4. Select one of the following methods to open the listener configuration wizard:
   - On the Server Load Balancer page, find the target SLB instance and then click Configure Listener in the Actions column.
   - On the Server Load Balancer page, click the ID of the target SLB instance. On the Listeners tab, click Add Listener.

Step 2 Configure the UDP listener

To configure the UDP listener, follow these steps:

1. On the Protocol and Listener page, configure the UDP listener according to the following information.

Configuration	Description
Select Listener Protocol	Select the protocol type of the listener. In this topic, select UDP.

Configuration	Description
Listening Port	The listening port used to receive requests and forward the requests to backend servers. The port number is in the range of 1 to 65535. Note: In the same SLB instance, the UDP or TCP listener port numbers can be the same in the following regions. However, you must first apply for the privilege to use the beta function of configuring the same ports in TCP/UDP listeners on the Quota Management page of the SLB console. In other cases, the listener port numbers must be unique. · UAE (Dubai) · Australia (Sydney) · UAE (Dubai) · UK (London) · Germany (Frankfurt) · US (Silicon Valley) · US (Virginia) · Indonesia (Jakarta) · Japan (Tokyo) · India (Mumbai) · Singapore · Malaysia (Kuala Lumpur) · China (Hong Kong) · China (Shenzhen) · China (Hohhot) · China (Qingdao) · China (Chengdu) · China (Zhangjiakou) · China (Shanghai)
Advanced configurations	

Configuration	Description
Scheduling Algorithm	SLB supports four scheduling algorithms: round robin, weighted round robin (WRR), weighted least connections (WLC), and consistent hash. · Weighted Round-Robin (WRR): A backend server with a higher weight receives more requests. · Round-Robin (RR): Requests are evenly and sequentially distributed to backend servers. · Weighted Least Connections (WLC): A server with a higher weight receives more requests. When the weight values of two backend servers are the same, the backend server with a smaller number of connections is more likely to be polled. · Consistent Hash (CH): - Source IP: the consistent hash based on source IP addresses. Requests from the same source IP address are scheduled to the same backend server. - Tuple: the consistent hash based on four factors: source IP address + destination IP address + source port + destination port. The same streams are scheduled to the same backend server. - QUIC ID: the consistent hash based on the QUIC Connection ID. The same QUIC Connection IDs are scheduled to the same backend server. Notice: The QUIC protocol is rapidly evolving. The algorithm is based on draft-ietf-quic-transport-10 and does not guarantee the compatibility of all QUIC versions. We recommend that you do enough tests before using it for the production environment. Note: Currently, the Consistent Hash (CH) algorithm is only supported in the following regions: - Japan (Tokyo) - Australia (Sydney) - Malaysia (Kuala Lumpur) - Indonesia (Jakarta) - Germany (Frankfurt)

Configuration	Description
Enable Access Control	Select whether to enable the access control function.
Access Control Method	Select an access control method after you enable the access control function: · Whitelist: Only requests from IP addresses or CIDR blocks in the selected access control list are forwarded. It applies to scenarios where the application only allows access from some specific IP addresses. Enabling a whitelist poses some risks to your services. After a whitelist is configured, only the IP addresses in the list can access the listener. If you enable the whitelist without adding any IP addresses in the corresponding access control list, all requests are forwarded. · Blacklist: Requests from IP addresses or CIDR blocks in the selected access control list are not forwarded. It applies to scenarios where the application only denies access from some specific IP addresses. If you enable a blacklist without adding any IP addresses in the corresponding access control list, all requests are forwarded.
Access Control List	Select an access control list as the whitelist or the blacklist.  Note: An IPv6 instance can only be associated with IPv6 access control lists and an IPv4 instance can only be associated with IPv4 access control lists. For more information, see Configure an access control list.

Configuration	Description
Enable Peak Bandwidth Limit	Select whether to configure the listener bandwidth. If the SLB instance is charged based on bandwidth, you can set different peak bandwidth values for different listeners to limit the traffic passing through each listener. The sum of the peak bandwidth values of all listeners under an SLB instance cannot exceed the bandwidth value of that SLB instance. By default, all listeners share the bandwidth of the SLB instance. Note: SLB instances billed by traffic have no bandwidth peak limit by default.
Get Client Source IP Address	Backend servers of a UDP listener can directly obtain source IP addresses of clients. Note: UDP listeners of an SLB instance of the classic network do not support viewing source IP addresses.
Automatically Enable Listener After Creation	Choose whether to start the listener after the listener is configured. The listener is started by default.

2. Click Next.

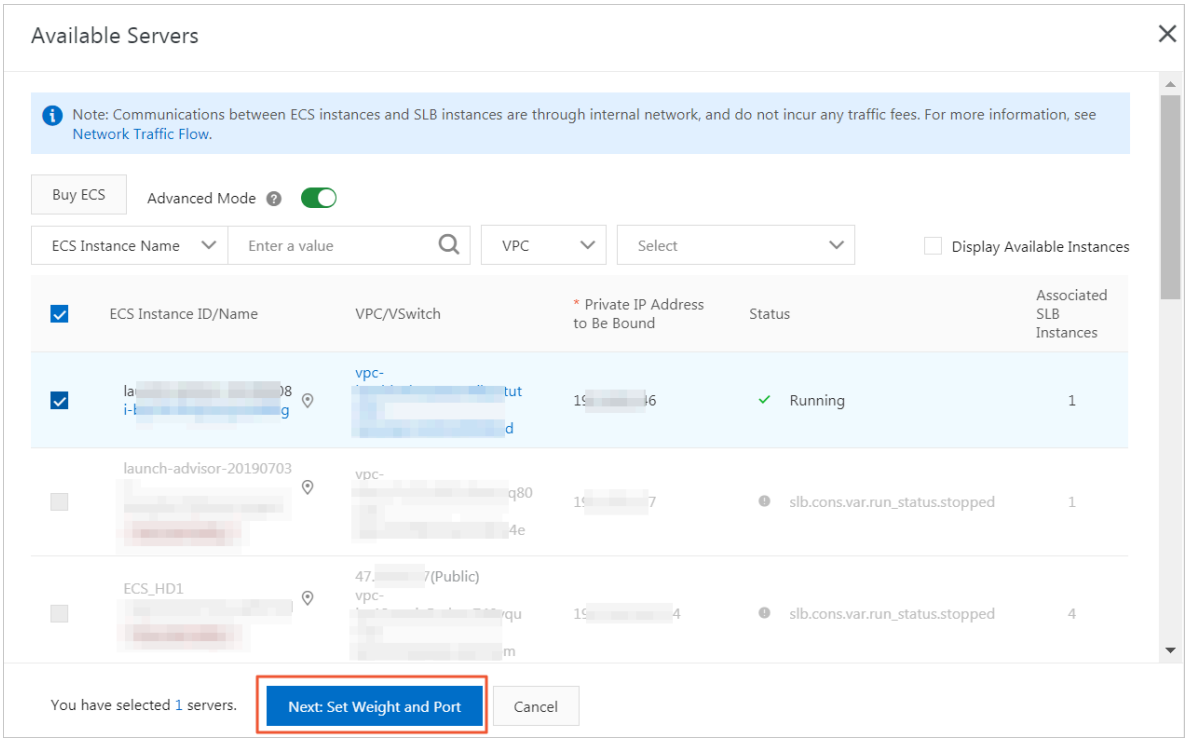
Step 3 Add backend servers

After configuring the listener, you need to add backend servers to process requests. You can use the default server group configured for the SLB instance, or configure a VServer group or an active/standby server group for the listener. For more information, see #unique_12.

In this example, use the default server group.

1. Select Default Server Group and then click Add More.

2. Select the ECS instances to add, and then click Next: Set Weight and Port.



3. Configure ports and weights for the added backend servers (ECS instances).

   - Port

     The port opened on the backend server to receive requests. The port number is in the range of 1 to 65535. Ports of backend servers can be the same in an SLB instance.

   - Weight

     The weight of the backend server. A backend server with a higher weight receives more requests.

     > **Note:**
     > If the weight is set to 0, no requests are sent to the backend server.

4. Click Next.

Step 4 Configure health checks

SLB checks the service availability of backend servers by performing health checks. The health check function improves the overall availability of your services and avoids the impact of backend server failures. Click Modify to change health check configurations. For more information, see #unique_13.

Step 5 Submit the configurations

To submit the listener configurations, follow these steps:

1. On the Submit page, check the listener configurations. You can click Modify to change the configurations.
2. Click Submit.
3. On the Submit page, click OK after the configurations are successful.

   After the configurations are successful, you can view the created listener on the Listeners page.

#unique_14

#unique_15

#unique_16

#unique_20

#unique_17

#unique_21

4 Add an HTTP listener

This topic describes how to add an HTTP listener to a Server Load Balancer (SLB) instance. You can add an HTTP listener to forward requests from the HTTP protocol.

Prerequisites

An SLB instance is created. For more information, see #unique_10.

Step 1 Open the listener configuration wizard

To open the listener configuration wizard, follow these steps:

1. Log on to the Server Load Balancer console.
2. In the left-side navigation pane, choose Instances > Server Load Balancer.
3. Select the region of the target SLB instance.
4. Select one of the following methods to open the listener configuration wizard:
   - On the Server Load Balancer page, find the target SLB instance and then click Configure Listener in the Actions column.
   - On the Server Load Balancer page, click the ID of the target SLB instance. On the Listeners tab, click Add Listener.

Step 2 Configure the HTTP listener

To configure the HTTP listener, follow these steps:

1. On the Protocol and Listener page, configure the HTTP listener according to the following information:

Configuration	Description
Select Listener Protocol	Select the protocol type of the listener. In this topic, select HTTP.

Configuration	Description
Listening Port	The listening port used to receive requests and forward the requests to backend servers. Value range: 1 to 65535. Note: The listening port must be unique in an SLB instance.
Advanced configurations	
Scheduling Algorithm	SLB supports three scheduling algorithms: round robin, weighted round robin (WRR), and weighted least connections (WLC). · Weighted Round-Robin (WRR): A backend server with a higher weight receives more requests. · Round-Robin (RR): Requests are evenly and sequentially distributed to backend servers. · Weighted Least Connections (WLC): A server with a higher weight receives more requests. When the weight values of two backend servers are the same, the backend server with a smaller number of connections is more likely to be polled.
Redirection	Select whether to forward traffic of the HTTP listener to an HTTPS listener. Note: Before you enable the redirection function, make sure that you have created an HTTPS listener.

Configuration	Description
Session Persistence	Select whether to enable session persistence. After you enable session persistence, all session requests from the same client are sent to the same backend server. HTTP session persistence is based on cookies. The following two methods are supported: · Insert cookie: You only need to specify the cookie timeout period. SLB adds a cookie to the first response from the backend server (inserts SERVERID in the HTTP and HTTPS response packet). The next request will contain the cookie and the listener will distribute the request to the same backend server. · Rewrite cookie: You can set the cookie to insert to the HTTP or HTTPS response according to your needs. You must maintain the timeout period and lifecycle of the cookie on the backend server. SLB will overwrite the original cookie when it discovers that a new cookie is set. The next time the client carries the new cookie to access SLB, the listener will distribute the request to the recorded backend server. For more information, see Session persistence.
Enable Access Control	Select whether to enable the access control function.

Configuration	Description
Access Control Method	Select an access control method after you enable the access control function: · Whitelist: Only requests from IP addresses or CIDR blocks in the selected access control list are forwarded. It applies to scenarios where the application only allows access from some specific IP addresses. Enabling a whitelist poses some risks to your services. After a whitelist is configured, only the IP addresses in the list can access the listener. If you enable the whitelist without adding any IP addresses in the corresponding access control list, all requests are forwarded. · Blacklist: Requests from IP addresses or CIDR blocks in the selected access control list are not forwarded. It applies to scenarios where the application only denies access from some specific IP addresses. If you enable a blacklist without adding any IP addresses in the corresponding access control list, all requests are forwarded.
Access Control List	Select an access control list as the whitelist or the blacklist. Note: An IPv6 instance can only be associated with IPv6 access control lists and an IPv4 instance can only be associated with IPv4 access control lists. For more information, see Configure an access control list.

Configuration	Description
Enable Peak Bandwidth Limit	Select whether to configure the listener bandwidth. If the SLB instance is charged based on bandwidth , you can set different peak bandwidth values for different listeners to limit the traffic passing through each listener. The sum of the peak bandwidth values of all listeners under an SLB instance cannot exceed the bandwidth value of that SLB instance. By default, all listeners share the bandwidth of the SLB instance.  Note: SLB instances billed by traffic have no peak bandwidth limit by default.
Idle Timeout	Specify the idle connection timeout period. Value range: 1 to 60. Unit: seconds. If no request is received during the specified timeout period, SLB temporarily terminates the connection and restarts the connection when the next request is received. Currently, this function is available in all regions.  Note: This function does not work for HTTP/2.0 requests.
Request Timeout	Specify the request timeout period. Value range: 1 to 180. Unit: seconds. If no response is received from the backend server during the specified timeout period, SLB stops waiting and sends an HTTP 504 error code to the client. Currently, this function is available in all regions.

Configuration	Description
Enable Gzip Compression	Choose whether to enable Gzip compression to compress files of specific formats. Now Gzip supports the following file types: text/xml, text/plain, text/css, application/javascript, application/x-javascript, application/rss+xml, application/atom+xml, and application/xml.
Add HTTP Header Fields	Select the custom HTTP headers that you want to add: · Use the `X-Forwarded-For` field to retrieve client source IP addresses. · Use the `X-Forwarded-Proto` field to retrieve the listener protocol used by the SLB instance. · Use the `SLB-IP` field to retrieve the public IP address of the SLB instance. · Use the `SLB-ID` field to retrieve the ID of the SLB instance.
Get Client Source IP Address	HTTP listeners use X-Forwarded-For to obtain real IP addresses of clients.
Automatically Enable Listener After Creation	Choose whether to start the listener after the listener is configured. The listener is started by default.

2. Click Next.

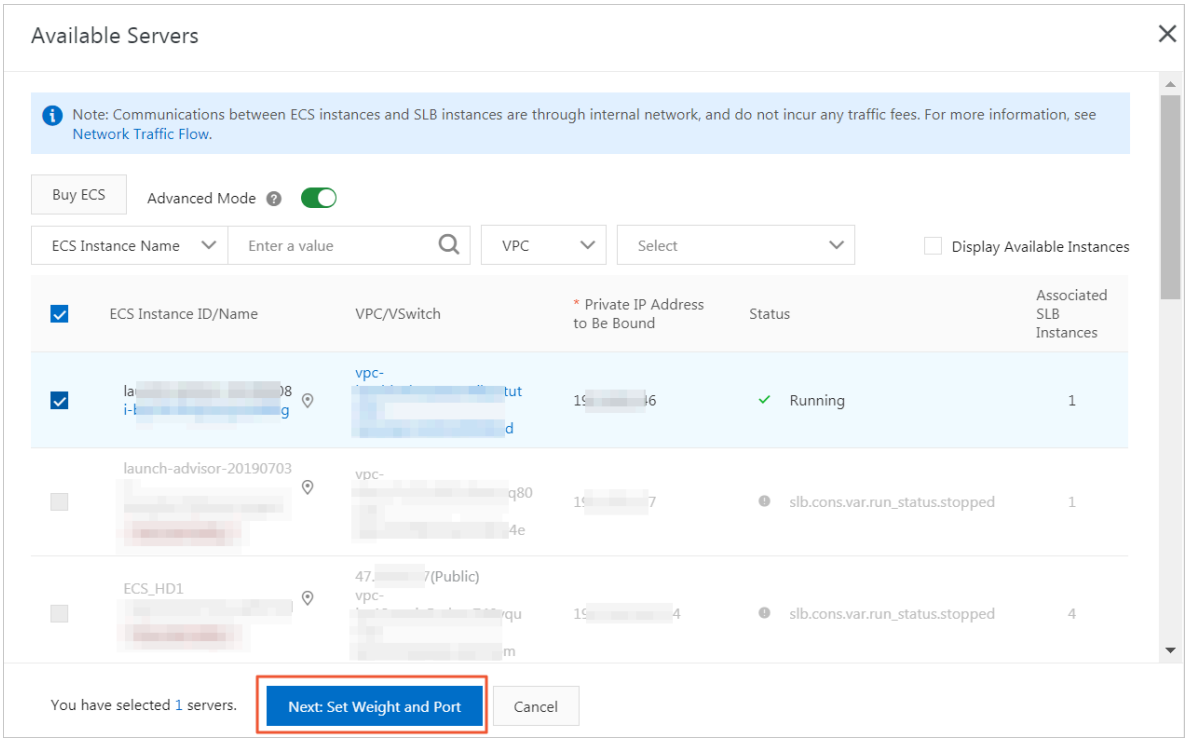
Step 3 Add backend servers

After configuring the listener, you need to add backend servers to process requests. You can use the default server group configured for the SLB instance, or configure a VServer group or an active/standby server group for the listener. For more information, see #unique_12.

In this example, use the default server group.

1. Select Default Server Group and then click Add More.

2. Select the ECS instances to add, and then click Next: Set Weight and Port.



3. Configure ports and weights for the added backend servers (ECS instances).

   - Port

     The port opened on the backend server to receive requests. The port number is in the range of 1 to 65535. Ports of backend servers can be the same in an SLB instance.

   - Weight

     The weight of the backend server. A backend server with a higher weight receives more requests.

     > **Note:**
     > If the weight is set to 0, no requests are sent to the backend server.

4. Click Next.

Step 4 Configure health checks

SLB checks the service availability of backend servers by performing health checks. The health check function improves the overall availability of your services and avoids the impact of backend server failures. Click Modify to change health check configurations. For more information, see #unique_13.

Step 5 Submit the configurations

To submit the listener configurations, follow these steps:

1. On the Submit page, check the listener configurations. You can click Modify to change the configurations.
2. Click Submit.
3. On the Submit page, click OK after the configurations are successful.

   After the configurations are successful, you can view the created listener on the Listeners page.

#unique_14

#unique_15

#unique_16

#unique_20

#unique_17

#unique_24

#unique_25

#unique_26

5 Add an HTTPS listener

This topic describes how to add an HTTP listener to a Server Load Balancer (SLB) instance. You can add an HTTPS listener to forward requests from the HTTPS protocol.

Prerequisites

An SLB instance is created. For more information, see #unique_10.

Step 1 Open the listener configuration wizard

To open the listener configuration wizard, follow these steps:

1. Log on to the Server Load Balancer console.
2. In the left-side navigation pane, choose Instances > Server Load Balancer.
3. Select the region of the target SLB instance.
4. Select one of the following methods to open the listener configuration wizard:
   - On the Server Load Balancer page, find the target SLB instance and then click Configure Listener in the Actions column.
   - On the Server Load Balancer page, click the ID of the target SLB instance. On the Listeners tab, click Add Listener.

Step 2 Configure the HTTPS listener

To configure the HTTPS listener, follow these steps:

1. On the Protocol and Listener page, configure the HTTPS listener according to the following information:

Configuration	Description
Select Listener Protocol	Select the protocol type of the listener. In this topic, select HTTPS.

Configuration	Description
Listening Port	The listening port used to receive requests and forward the requests to backend servers. Value range: 1 to 65535 Note: The listening port must be unique in an SLB instance.
Advanced configurations	
Scheduling Algorithm	SLB supports three scheduling algorithms: round robin, weighted round robin (WRR), and weighted least connections (WLC). · Weighted Round-Robin (WRR): A backend server with a higher weight receives more requests. · Round-Robin (RR): Requests are evenly and sequentially distributed to backend servers. · Weighted Least Connections (WLC): A server with a higher weight receives more requests. When the weight values of two backend servers are the same, the backend server with a smaller number of connections is more likely to be polled.

Configuration	Description
Enable Session Persistence	Select whether to enable session persistence. After you enable session persistence, all session requests from the same client are sent to the same backend server. HTTP session persistence is based on cookies. The following two methods are supported: · Insert cookie: You only need to specify the cookie timeout period. SLB adds a cookie to the first response from the backend server (inserts SERVERID in the HTTP and HTTPS response packet). The next request will contain the cookie and the listener will distribute the request to the same backend server. · Rewrite cookie: You can set the cookie to be inserted to the HTTP or HTTPS response according to your needs. You must maintain the timeout period and lifecycle of the cookie on the backend server. SLB will overwrite the original cookie when it discovers that a new cookie is set. The next time the client carries the new cookie to access SLB, the listener will distribute the request to the recorded backend server. For more information, see Configure session persistence.
Enable HTTP/2	Select whether to enable HTTP 2.0.
Enable Access Control	Select whether to enable the access control function.

Configuration	Description
Access Control Method	Select an access control method after you enable the access control function: · Whitelist: Only requests from IP addresses or CIDR blocks in the selected access control list are forwarded. It applies to scenarios where the application only allows access from some specific IP addresses. Enabling a white access control list poses some risks to your services. After a whitelist is configured, only the IP addresses in the list can access the listener. If you enable the whitelist without adding any IP addresses in the corresponding access control list, all requests are forwarded. · Blacklist: Requests from IP addresses or CIDR blocks in the selected access control list are not forwarded. It applies to scenarios where the application only denies access from some specific IP addresses. If you enable a blacklist without adding any IP addresses in the corresponding access control list, all requests are forwarded.
Access Control List	Select an access control list as the whitelist or the blacklist. Note: An IPv6 instance can only be associated with IPv6 access control lists and an IPv4 instance can only be associated with IPv4 access control lists. For more information, see Configure an access control list.

Configuration	Description
Enable Peak Bandwidth Limit	Select whether to configure the listening bandwidth. If the SLB instance is charged based on bandwidth , you can set different peak bandwidth values for different listeners to limit the traffic passing through each listener. The sum of the peak bandwidth values of all listeners under an SLB instance cannot exceed the bandwidth value of that SLB instance. By default, all listeners share the bandwidth of the SLB instance. Note: SLB instances billed by traffic have no peak bandwidth limit by default.
Idle Timeout	Specify the idle connection timeout period. Value range: 1 to 60. Unit: seconds. If no request is received during the specified timeout period, SLB temporarily terminates the connection and restarts the connection when the next request is received. This function is available in all regions.
Request Timeout	Specify the request timeout period. Value range: 1 to 180. Unit: seconds. If no response is received from the backend server during the specified timeout period, SLB stops waiting and sends an HTTP 504 error code to the client. Currently, this function is available in all regions.

Configuration	Description
TLS Security Policy	Only guaranteed-performance instances support selecting the TLS security policy. The TLS security policy contains available TLS protocol versions and supported cipher suites. For more information, see #unique_28.
Enable Gzip Compression	Choose whether to enable Gzip compression to compress files of specific formats. Now Gzip supports the following file types: text/xml, text/plain, text/css, application/javascript, application/x-javascript, application/rss+xml, application/atom+xml, and application/xml.
Add HTTP Header Fields	Select the custom HTTP headers that you want to add: · Use the `X-Forwarded-For` field to retrieve client source IP addresses. · Use the `X-Forwarded-Proto` field to retrieve the listener protocol used by the SLB instance. · Use the `SLB-IP` field to retrieve the public IP address of the SLB instance. · Use the `SLB-ID` field to retrieve the ID of the SLB instance.
Get Client Source IP Address	HTTP listeners use X-Forwarded-For to obtain real IP addresses of clients.
Automatically Enable Listener After Creation	Choose whether to start the listener after the listener is configured. The listener is started by default.

2. Click Next.

Step 3 Configure the SSL certificate

To add an HTTPS listener, you must upload a server certificate or CA certificate, as shown in the following table.

Certificate	Description	Required for one-way authentication?	Required for mutual authentication?
Server certificate	Used to identify a server. The client uses it to check whether the certificate sent by the server is issued by a trusted center.	Yes. You need to upload the server certificate to the certificate management system of SLB.	Yes. You need to upload the server certificate to the certificate management system of SLB.
Client certificate	Used to identify a client. The client user can prove its true identity when communicating with the server. You can sign a client certificate with a self-signed CA certificate.	No.	Yes. You need to install the client certificate on the client.
CA certificate	The server uses the CA certificate to authenticate the signature on the client certificate, as part of the authentication before launching a secure connection. If the authentication fails, the connection is rejected.	No.	Yes. You need to upload the CA certificate to the certificate management system of SLB.

Note the following before you upload a certificate:

- The uploaded certificate must be in the PEM format. For more information, see #unique_29.
- After the certificate is uploaded to SLB, SLB can manage the certificate and you do not need to associate the certificate with backend ECS instances.
- It usually takes one to three minutes to activate the HTTPS listener because the uploading, loading, and validation of certificates take some time. Normally it takes effect in one minute and it will definitely take effect in three minutes.
- The ECDHE algorithm cluster used by HTTPS listeners supports forward secrecy, but does not support uploading security enhancement parameter files required

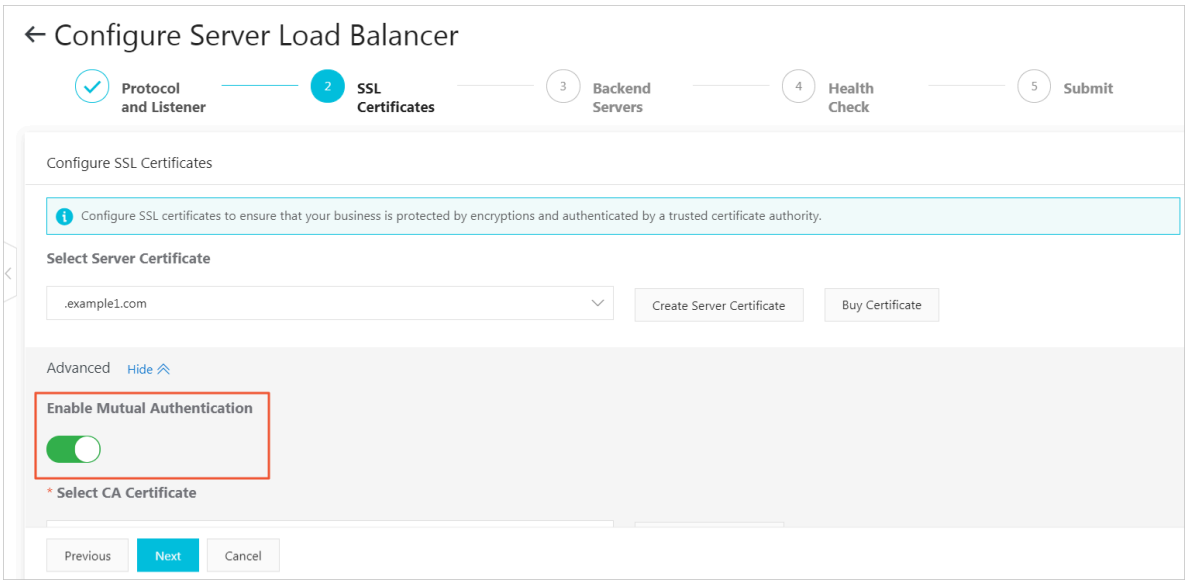
by the DHE algorithm cluster, such as strings containing the `BEGIN DH PARAMETERS` field in the PEM certificate file. For more information, see Certificate requirements.

- Currently, SLB HTTPS listeners do not support SNI (Server Name Indication). You can use TCP listeners instead, and then configure SNI on backend ECS instances.
- The session ticket timeout period of HTTPS listeners is 300 seconds.
- The actual amount of traffic is larger than the billed traffic amount because some traffic is used for protocol handshaking.
- In the case of a large number of new connections, HTTPS listeners consume more traffic.

1. Select the server certificate that has been uploaded, or click Create Server Certificate to upload a server certificate.

   For more information, see #unique_31.

2. If you want to enable HTTPS mutual authentication or set a TLS security policy, click Modify.



3. Select an uploaded CA certificate, or click Create CA Certificate to upload a CA certificate.

   You can use a self-signed CA certificate. For more information, see #unique_31.

4. Select a TLS security policy. For more information, see #unique_28.

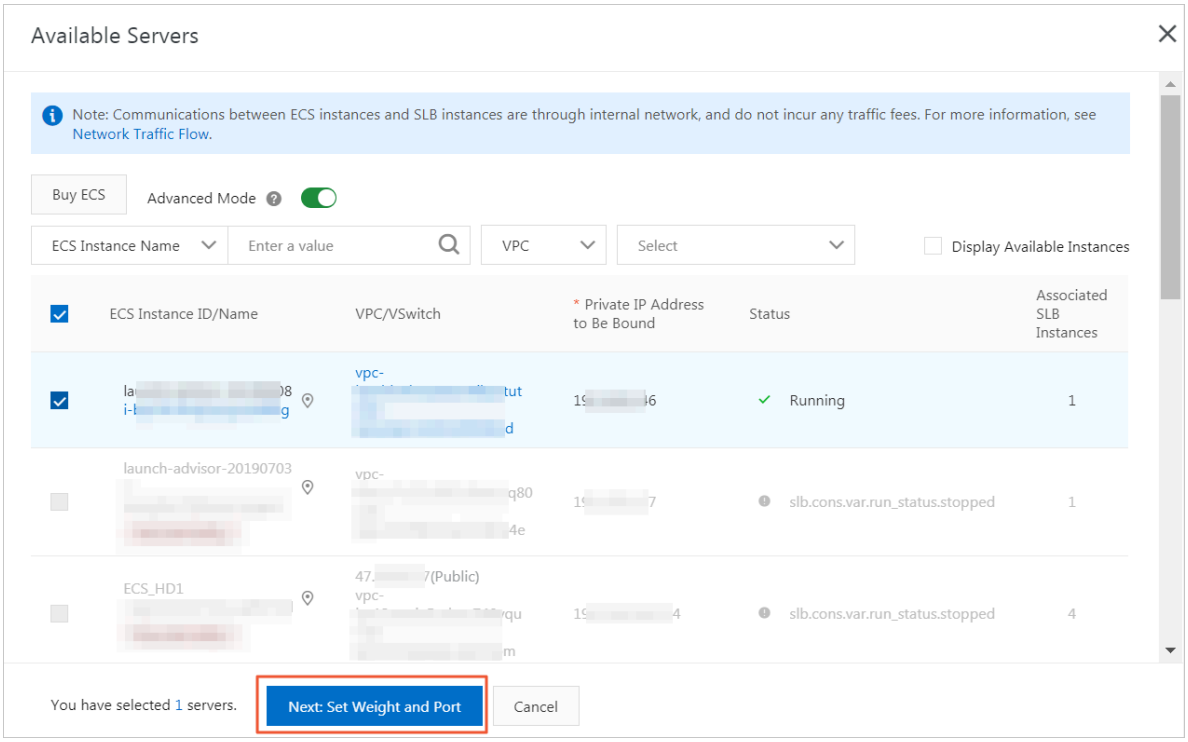
Step 4 Add backend servers

You need to add backend servers to process requests. You can use the default server group configured for the SLB instance, or configure a VServer group or an active/standby server group for the listener. For more information, see #unique_12.

In this topic, use the default server group.

1. Select Default Server Group and then click Add More.

2. Select the ECS instances to add, and then click Next: Set Weight and Port.



3. Configure ports and weights for the added backend servers (ECS instances).

   - Port

     The port opened on the backend server to receive requests. The port number is in the range of 1 to 65535. Ports of backend servers can be the same in an SLB instance.

   - Weight

     The weight of the backend server. A backend server with a higher weight receives more requests.

> **Note:**

If the weight is set to 0, no requests are sent to the backend server.

4. Click Next.

Step 5 Configure health checks

SLB checks the service availability of backend servers by performing health checks. The health check function improves the overall availability of your services and avoids the impact of backend server failures. Click Modify to change health check configurations. For more information, see #unique_13.

Step 6 Submit the configurations

To submit the listener configurations, follow these steps:

1. On the Submit page, check the listener configurations. You can click Modify to change the configurations.
2. Click Submit.
3. On the Submit page, click OK after the configurations are successful.

   After the configurations are successful, you can view the created listener on the Listeners page.

#unique_14

#unique_15

#unique_16

#unique_20

#unique_17

#unique_24

#unique_25

#unique_32

6 Domain name extensions

6.1 Manage a domain name extension

HTTPS listeners of guaranteed-performance Server Load Balancer (SLB) instances support configuring multiple certificates, allowing you to forward requests with different domain names to different backend servers.

Introduction to SNI

Server Name Indication (SNI) is an extension to the SSL/TLS protocol, allowing a server to install multiple SSL certificates on the same IP address. When a client accesses SLB, the certificate configured for the domain name is used by default. If no certificate is configured for the domain name, the certificate configured for the HTTPS listener is used.

 Note:
Only guaranteed-performance SLB instances support SNI.

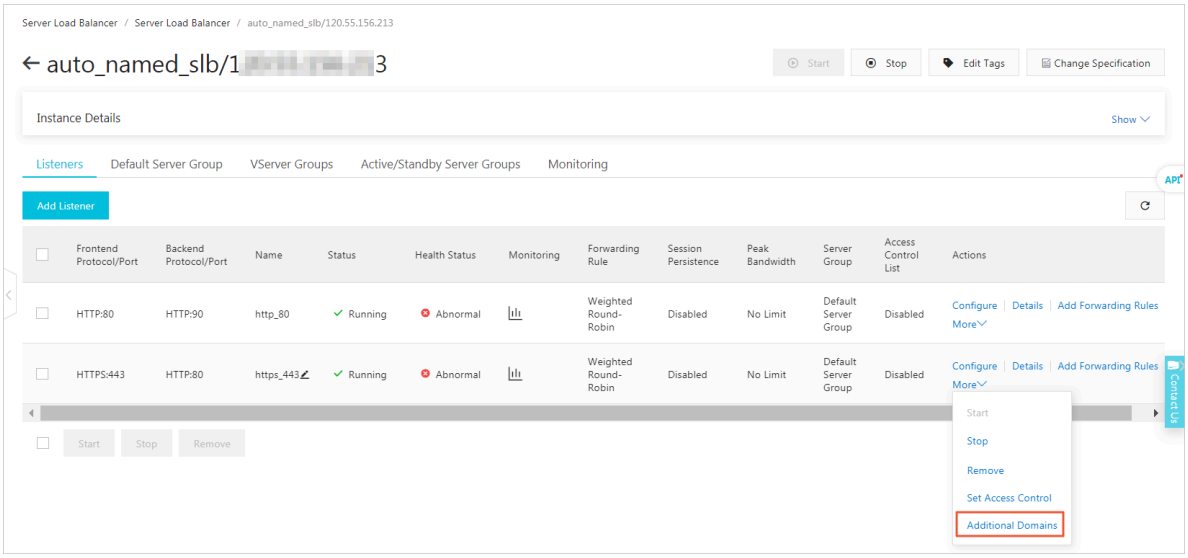
If you want to resolve multiple domain names to the IP address of an SLB instance, distribute requests from different domains to different backend servers, and at the same time use HTTPS encrypted access, you can use the domain name extension function.

The domain name extension function is available in all regions.

Add a domain name extension

1. Log on to the SLB console.
2. Select the region of the target SLB instance.
3. Find the target SLB instance and click the instance ID.
4. Click the Listeners tab.

5. On the Listeners tab page, find the target HTTPS listener, and choose More > Additional Domains in the Actions column.



6. Click Add Additional Domain and configure the domain name:

   a. Enter a domain name. The domain name can only contain letters, numbers, hyphens (-), and periods (.), and must start with a letter or a number. To check if the domain name you enter is valid, you can use the Alibaba Cloud domain name check tool.

      Domain name-based forwarding rules support exact match and wildcard match.

      - Exact domain name: www.aliyun.com
      - Wildcard domain name (generic domain name): *.aliyun.com, *.market.aliyun.com

      When a request matches multiple forwarding rules, exact match takes precedence over small-scale wildcard match and small-scale wildcard match takes precedence over large-scale wildcard match, as shown in the following table.

Type	Request URL	Request URL		
		www.aliyun.com	*.aliyun.com	*.market.aliyun.com
Exact match	www.aliyun.com	√	×	×
Wildcard match	market.aliyun.com	×	√	×

Type	Request URL	Request URL		
		www.aliyun.com	*.aliyun.com	*.market.aliyun.com
Wildcard match	info.market.aliyun.com	×	×	√

b. Select the certificate associated with the domain name.

> Note:
> The domain name in the certificate must be the same as the added domain name extension.

c. Click OK.

7. On the Listeners page, find the target HTTPS listener and click Add Forwarding Rules in the Actions column.
8. On the Add Forwarding Rules page, configure the forwarding rule and click Add Forwarding Rules.
9. For more information, see #unique_24.

> Note:
> Make sure that the domain name configured in the forwarding rule is the same as the added domain name extension.

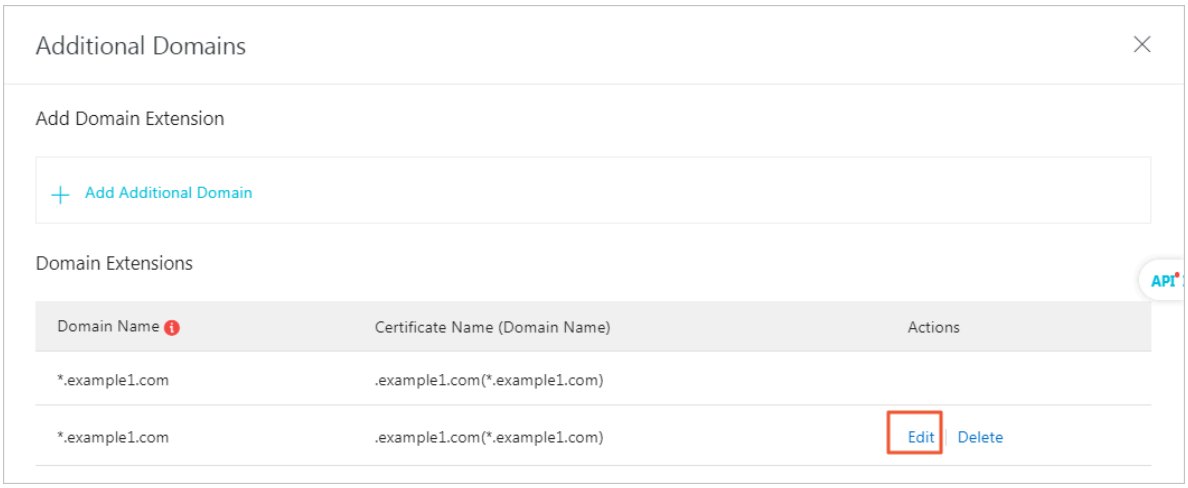
Edit a domain name extension

You can replace the certificate used by an added domain name extension.

To edit a domain name extension, follow these steps:

1. Log on to the SLB console.
2. Select the region of the target SLB instance.
3. Find the target SLB instance and click the instance ID.
4. Click the Listeners tab.
5. On the Listeners page, find the created HTTPS listener, and then choose More > Additional Domains in the Actions column.
6. Find the target domain name extension and then click Edit.

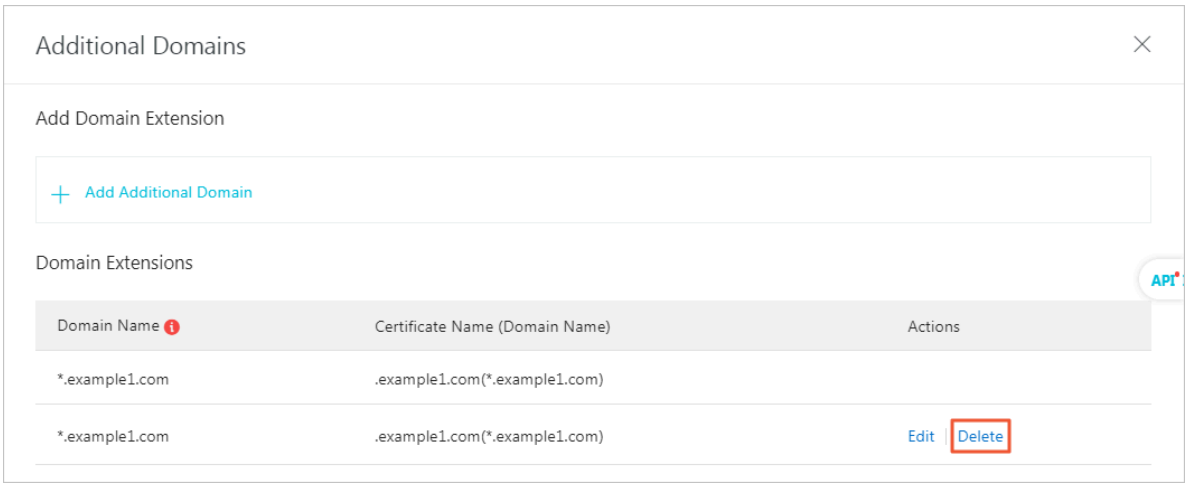
7. In the Edit Additional Domain dialog box, select a new certificate and then click OK.



Delete a domain name extension

To delete a domain name extension, follow these steps:

1. Log on to the SLB console.
2. Select the region of the target SLB instance.
3. Find the target SLB instance and click the instance ID.
4. Click the Listeners tab.
5. On the Listeners page, find the created HTTPS listener, and then choose More > Additional Domains in the Actions column.
6. Find the target domain name extension and click Delete.



7. In the displayed dialog box, click OK.

6.2 Add a domain name extension

This topic describes how to add a domain name extension.

Procedure

1. Log on to the Server Load Balancer console.
2. Select the region of the target SLB instance.
3. Find the target SLB instance and click the instance ID.
4. Click the Listeners tab.
5. On the Listeners tab, find the target HTTPS listener, and choose More > Additional Domains in the Actions column.

6. Click Add Additional Domain and configure the domain name:
   a) Enter a domain name. The domain name can only contain letters, numbers, hyphens (-), and periods (.), and must start with a letter or a number. To check if the domain name you enter is valid, you can use the Alibaba Cloud domain name check tool.

      Domain name-based forwarding rules support exact match and wildcard match.

      - Exact domain name: www.aliyun.com
      - Wildcard domain name (generic domain name): *.aliyun.com, *.market.aliyun.com

      When a request matches multiple forwarding rules, exact match takes precedence over small-scale wildcard match and small-scale wildcard match takes precedence over large-scale wildcard match, as shown in the following table.

Type	Request URL	Domain name-based forwarding rule		
		www.aliyun.com	*.aliyun.com	*.market.aliyun.com
Exact match	www.aliyun.com	√	×	×
Wildcard match	market.aliyun.com	×	√	×

Type	Request URL	Domain name-based forwarding rule		
		www.aliyun.com	*.aliyun.com	*.market.aliyun.com
Wildcard match	info.market.aliyun.com	×	×	√

b) Select the certificate associated with the domain name.

> Note:
> The domain name in the certificate must be the same as the added domain name extension.

c) Click OK.

7. On the Listeners tab, find the target HTTPS listener and click Add Forwarding Rules in the Actions column.
8. On the Add Forwarding Rules page, configure the forwarding rule and click Add Forwarding Rules.
9. For more information, see #unique_24.

> Note:
> Make sure that the domain name configured in the forwarding rule is the same as the added domain name extension.

More information
#unique_36

6.3 Edit a domain name extension

You can replace the certificate used by an added domain name extension.

Procedure

1. Log on to the Server Load Balancer console.
2. Select the region of the target SLB instance.
3. Find the target SLB instance and click the instance ID.
4. Click the Listeners tab.

5. On the Listeners tab, find the target HTTPS listener, and then choose More > Additional Domains in the Actions column.
6. Find the target domain name extension and then click Edit.
7. In the Edit Additional Domain dialog box, select a new certificate and then click OK.

6.4 Delete a domain name extension

You can delete a domain name extension when you no longer need it.

Procedure

1. Log on to the Server Load Balancer console.
2. Select the region of the target SLB instance.
3. Find the target SLB instance and click the instance ID.
4. Click the Listeners tab.
5. On the Listenerstab page, find the target HTTPS listener, and then choose More > Additional Domains in the Actions column.
6. Find the target domain name extension and click Delete.
7. In the displayed dialog box, click OK.

7 Manage TLS security policies

When you add or configure an HTTPS listener for a guaranteed-performance Server Load Balancer (SLB) instance, you can select from a variety of TLS security policies and apply one according to your requirements.

You can select a TLS security policy when you set advanced configurations of SSL Certificates for an HTTPS listener. For more information, see #unique_40.

A TLS security policy contains supported TLS protocol versions and cipher suites.

TLS security policy

Security policy	Feature	Supported TLS version	Supported cipher suite
tls_cipher_policy_1_0	Optimal compatibility and with basic security	TLSv1.0, TLSv1.1, and TLSv1.2	ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES256-GCM-SHA384, ECDHE-RSA-AES128-SHA256, ECDHE-RSA-AES256-SHA384, AES128-GCM-SHA256, AES256-GCM-SHA384, AES128-SHA256, AES256-SHA256, ECDHE-RSA-AES128-SHA, ECDHE-RSA-AES256-SHA, AES128-SHA, AES256-SHA, and DES-CBC3-SHA
tls_cipher_policy_1_1	Compatible and with standard security	TLSv1.1 and TLSv1.2	ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES256-GCM-SHA384, ECDHE-RSA-AES128-SHA256, ECDHE-RSA-AES256-SHA384, AES128-GCM-SHA256, AES256-GCM-SHA384, AES128-SHA256, AES256-SHA256, ECDHE-RSA-AES128-SHA, ECDHE-RSA-AES256-SHA, AES128-SHA, AES256-SHA, and DES-CBC3-SHA

Security policy	Feature	Supported TLS version	Supported cipher suite
tls_cipher_policy_1_2	Compatible and with advanced security	TLSv1.2	ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES256-GCM-SHA384, ECDHE-RSA-AES128-SHA256, ECDHE-RSA-AES256-SHA384, AES128-GCM-SHA256, AES256-GCM-SHA384, AES128-SHA256, AES256-SHA256, ECDHE-RSA-AES128-SHA, ECDHE-RSA-AES256-SHA, AES128-SHA, AES256-SHA, and DES-CBC3-SHA
tls_cipher_policy_1_2_strict	Supports only perfect forward secrecy (PFS) cipher suites and offers premium security.	TLSv1.2	ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES256-GCM-SHA384, ECDHE-RSA-AES128-SHA256, ECDHE-RSA-AES256-SHA384, ECDHE-RSA-AES128-SHA, and ECDHE-RSA-AES256-SHA

Security policy	Feature	Supported TLS version	Supported cipher suite
tls_cipher_policy_1_2_strict_with_1_3 Note: Currently, TLS1.3 is supported in the following regions: · UK (London) · China (Qingdao) · China (Hohhot) · China (Chengdu) · Japan (Tokyo) · India (Mumbai) · Australia (Sydney) · Malaysia (Kuala Lumpur) · US (Silicon Valley) · US (Virginia) · Germany (Frankfurt) · UAE (Dubai)	Supports only perfect forward secrecy (PFS) cipher suites and offers premium security.	TLS1.2 and TLS1.3	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, ECDHE -ECDSA-AES128-GCM-SHA256, ECDHE -ECDSA-AES256-GCM-SHA384, ECDHE-ECDSA-AES128-SHA256, ECDHE-ECDSA -AES256-SHA384, ECDHE-RSA-AES128 -GCM-SHA256, ECDHE-RSA-AES256 -GCM-SHA384, ECDHE-RSA-AES128-SHA256, ECDHE-RSA-AES256-SHA384 , ECDHE-ECDSA-AES128-SHA, ECDHE -ECDSA-AES256-SHA, ECDHE-RSA-AES128-SHA, and ECDHE-RSA-AES256-SHA

Algorithm support of different TLS security policies

Security policy		tls_cipher_policy_1_0	tls_cipher_policy_1_1	tls_cipher_policy_1_2	tls_cipher_policy_1_2_strict	tls_cipher_policy_1_2_strict_with_1_3
TLS	-	1.2/1.1/1.0	1.2/1.1	1.2	1.2	1.2 and 1.3
CIPHER	ECDHE-RSA-AES128-GCM-SHA256	#	#	#	#	#
	ECDHE-RSA-AES256-GCM-SHA384	#	#	#	#	#
	ECDHE-RSA-AES128-SHA256	#	#	#	#	#
	ECDHE-RSA-AES256-SHA384	#	#	#	#	#
	AES128-GCM-SHA256	#	#	#	-	-
	AES256-GCM-SHA384	#	#	#	-	-
	AES128-SHA256	#	#	#	-	-
	AES256-SHA256	#	#	#	-	-
	ECDHE-RSA-AES128-SHA	#	#	#	#	#
	ECDHE-RSA-AES256-SHA	#	#	#	#	#
	AES128-SHA	#	#	#	-	-
	AES256-SHA	#	#	#	-	-
	DES-CBC3-SHA	#	#	#	-	-
	TLS_AES_128_GCM_SHA256	-	-	-	-	#
	TLS_AES_256_GCM_SHA384	-	-	-	-	#

Security policy		tls_cipher_policy_1_0	tls_cipher_policy_1_1	tls_cipher_policy_1_2	tls_cipher_policy_1_2_strict	tls_cipher_policy_1_2_strict_with_1_3
	TLS_CHACHA20_POLY1305_SHA256	-	-	-	-	#
	TLS_AES_128_CCM_SHA256	-	-	-	-	#
	TLS_AES_128_CCM_8_SHA256	-	-	-	-	#
	ECDHE-ECDSA-AES128-GCM-SHA256	-	-	-	-	#
	ECDHE-ECDSA-AES256-GCM-SHA384	-	-	-	-	#
	ECDHE-ECDSA-AES128-SHA256	-	-	-	-	#
	ECDHE-ECDSA-AES256-SHA384	-	-	-	-	#
	ECDHE-ECDSA-AES128-SHA	-	-	-	-	#
	ECDHE-ECDSA-AES256-SHA	-	-	-	-	#

8 Redirect HTTP requests to HTTPS

HTTPS is the secure version of HTTP. With HTTPS, the data sent between the browser and the server is encrypted. Server Load Balancer (SLB) supports redirecting HTTP requests to HTTPS to facilitate whole-site HTTPS deployment. Redirecting HTTP requests to HTTPS is supported in all regions.

Prerequisites

An HTTPS listener is created. For more information, see #unique_40.

Context

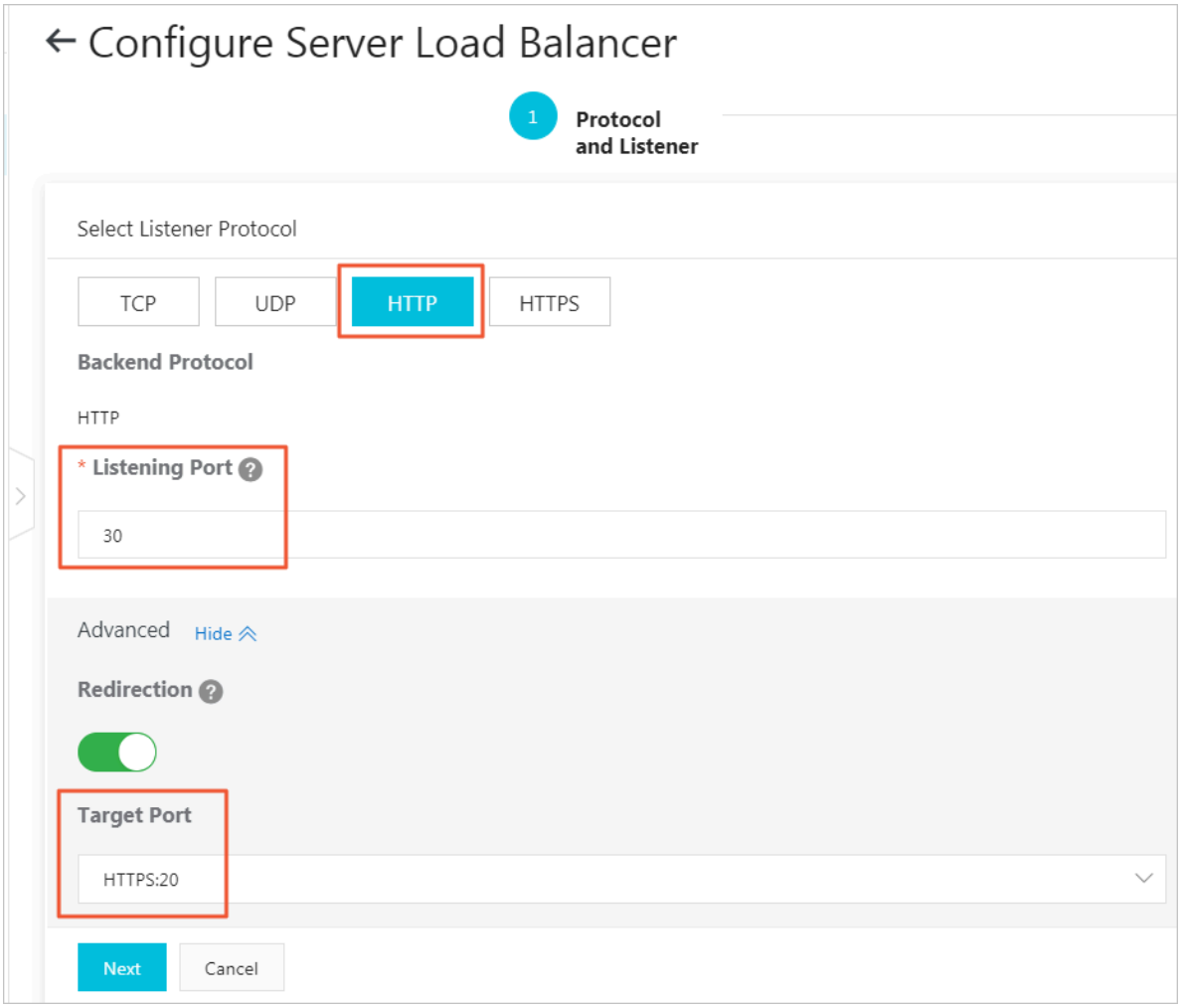
The redirection function is supported only by the new version SLB console.

Procedure

1. Log on to the SLB console.
2. Select the region of the target SLB instance.
3. On the Server Load Balancer page, click the ID of the target SLB instance.
4. Click the Listeners tab and then click Add Listener.
5. In the Configure Server Load Balancer dialog box, select HTTP as the listener protocol and configure the listening port.

6. In the Advanced section, turn on Redirection and select the target HTTPS listener.

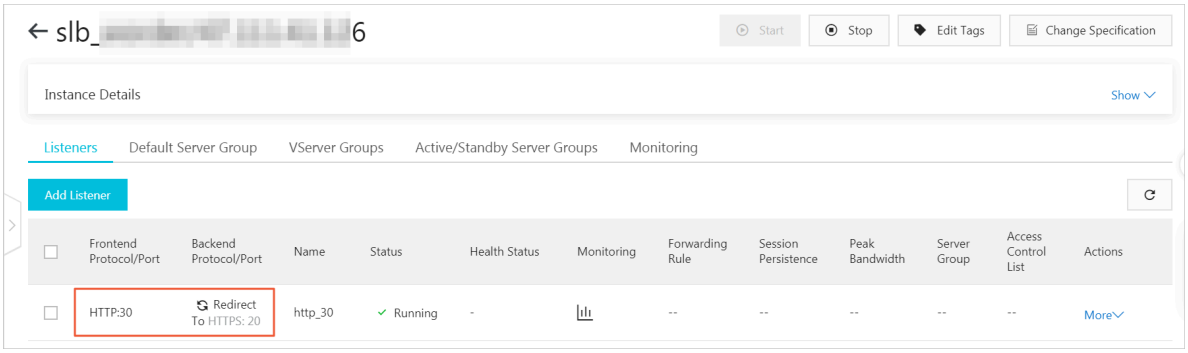
   The target listener can be an HTTPS listener with any port in the SLB instance.



7. Click Next.
8. Check the configurations and click Submit.

9. Click OK.

   After the redirection function is enabled, all HTTP requests will be redirected to the selected HTTPS listener and distributed according to the listener configurations of the HTTPS listener.



9 FAQ

9.1 HTTPS and HTTP listener FAQs

Why are some response header parameters deleted after requests are forwarded by Layer-7 listeners?

Symptoms: SLB modifies the values of the Date, Server, X-Pad, X-Accel-Redirect and other parameters in the response headers to achieve session persistence.

Solution:

- Add a prefix to the custom header, such as xl-server or xl-date.
- Change the Layer-7 listener to a Layer-4 listener.

Why is an additional header, namely the Transfer-Encoding: chunked, added to an HTTP request?

Symptoms: After a domain name is resolved into the IP address of a Layer-7 SLB instance, a Transfer-Encoding: chunked field is added in the HTTP request header when accessing the domain name from a local host. However, no such field is found in the request when accessing backend servers directly from the local host.

Layer-7 SLB is based on the Tengine reverse proxy. The Transfer-Encoding field indicates how the Web server encodes the response message body. For example, Transfer-Encoding: chunked indicates the chunked transfer encoding is used.

 Note:
This header is not added in the requests forwarded by Layer-4 listeners, because Layer-4 listeners only distribute traffic.

Why do the style sheets fail to load when I open a website through an HTTPS listener?

Symptoms:

An HTTP listener and an HTTPS listener are created respectively, and they use the same backend servers. When accessing the website over the HTTP listener with the specified port number, the website is displayed normally. However, the website layout is messy when accessing the website through the HTTPS listener.

Cause:

By default, SLB does not block loading and transferring JavaScript files. The possible reasons are as follows:

- The certificate is not compatible with the security level of the web browser.
- The certificate is an unqualified third-party certificate. In this case, contact the certificate issuer to check the certificate.

Solution:

1. When you open the website, click the prompt in the browser's address bar to load the script.
2. Add the required certificate to the browser.

Which port number do HTTPS listeners use?

There are no special requirements on ports. However, we recommend that you use 443 as the port number for HTTPS listeners.

What types of certificates does SLB support?

SLB supports uploading server certificates and CA certificates in the PEM format.

For the server certificates, you must upload both the certificate content and the private key. For the CA certificates, you only need to upload the certificate content.

Does SLB support keytool-created certificates?

Yes.

However, you must convert the certificate format to PEM before uploading the certificate to SLB. For more information, see Convert certificate format.

Can I use certificates in the PKCS#12(PFX) format?

Yes.

However, you must convert the certificate format to PEM before uploading the certificate to SLB. For more information, see Convert certificate format.

Why does a KeyEncryption error occur when uploading certificates?

The private key contains incorrect contents. For more information on private key format, see Certificate formats.

What SSL protocol versions are supported by the HTTPS Server Load Balancer service?

TLSv1, TLSv1.1, and TLSv1.2.

What is the lifetime of an HTTPS session ticket?

The lifetime of an HTTPS session ticket is set to 300 seconds.

Can I upload a certificate containing DH PARAMETERS?

No. The ECDHE method used by HTTPS listeners supports forward secrecy, but does not support uploading the PEM files that contain the security enhancement parameters, such as BEGIN DH PARAMETERS.

Do HTTPS listeners support SNI?

Yes. SNI (Server Name Indication) is an extension to SSL/TLS protocol so that a server can use multiple domain names and certificates. SLB HTTPS supports the SNI function. For more information, see #unique_47.

Which HTTP version is used by HTTP and HTTPS listeners to access the backend servers?

- When the protocol used by client requests is HTTP/1.1 or HTTP2/0, Layer-7 listeners use HTTP/1.1 to access backend servers.
- When the protocol used by client requests is neither HTTP/1.1 or HTTP2/0, Layer-7 listeners use HTTP/1.0 to access backend servers.

Can backend ECS instances obtain the protocol version used by the client to access the HTTP or HTTPS listener?

Yes.

What are the timeout values specified for HTTP and HTTPS listeners?

- A maximum of 100 requests can be sent continuously in an HTTP persistent connection. The connection is closed when the limit is reached.
- The timeout between two HTTP or HTTPS requests in an HTTP persistent connection is 15 seconds. The TCP connection is closed when the timeout exceeds 15 seconds. If you want to use the HTTP persistent connection, try to send heartbeat requests within 13 seconds.
- The timeout for the TCP three-way handshake between SLB and a backend ECS instance is 5 seconds. After the handshake times out, SLB selects the next ECS instance. You can find the timeout by checking the upstream response time in the access logs.
- The time that SLB waits for the response from an ECS instance is 60 seconds. If the wait time exceeds 60 seconds, a 504 or 408 status code is sent to the client. You can find the timeout by checking the upstream response time in the access logs.
- The HTTPS session reuse times out after 300 seconds. After the timeout, the client needs to perform the complete SSL handshake process again.