

Alibaba Cloud

Server Load Balancer
Access control

Document Version: 20220524

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 because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, 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 contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, 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 this document 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 directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
 Danger	A danger notice 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.
 Warning	A warning notice 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 restart an instance.
 Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: If the weight is set to 0, the server no longer receives new requests.
 Note	A note indicates supplemental instructions, best practices, tips, and other content.	 Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click Settings > Network > Set network type .
Bold	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click OK .
Courier font	Courier font is used for commands	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1.Overview	05
2.Access control lists	07
2.1. Create an access control list	07
2.2. Add IP entries	07
2.3. Delete IP entries	08
3.Enable access control	09
4.Disable access control	11

1. Overview

This topic describes how to enable access control for listeners of Server Load Balancer (SLB). You can configure access control when you create a listener or modify access control settings for created listeners.

Access control list

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

- **Whitelist:** The listener forwards only requests from IP addresses or CIDR blocks in the selected access control list. Use this list to allow only specified IP addresses to access your service.

The whitelist poses risks to your services. If you set the whitelist without adding any IP addresses to the selected access control list, the SLB listener does not forward any request.

- **Blacklist:** The listeners blocks only requests from IP addresses or CIDR blocks in the selected access control list. Use this list to forbid specified IP addresses to access your service.

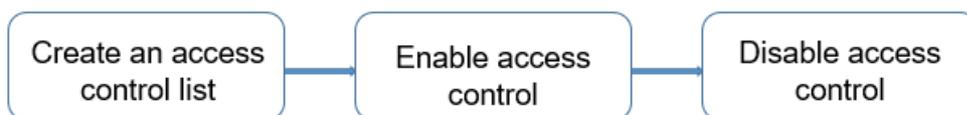
If you set the blacklist without adding any IP addresses to the selected access control list, the SLB listener forwards all requests.

Limits

- You can bind one or more access control lists to each SLB listener. By default, you can bind up to three access control lists to a listener in one of the following regions. You can bind only one access control list to a listener in a region that is not specified in the following list.
 - India (Mumbai)
 - Indonesia (Jakarta)
 - Japan (Tokyo)
 - Germany (Frankfurt)
 - Australia (Sydney)
 - Malaysia (Kuala Lumpur)
 - UK (London)
- You can bind only IPv4 access control lists to IPv4 SLB instances and only IPv6 access control lists to IPv6 SLB instances.
- The total sum of entries added to access control lists that are bound to the same listener must not exceed 1,000.
- An access control list can be bound to up to 50 listeners.
- The IP addresses in access control lists that are bound to the same listener must be unique.

Procedure

The following figure shows how to configure access control for listeners.



To configure access control for a listener, follow these steps:

- Create an access control list and add IP addresses or CIDR blocks to the list. For more information, see

[Create an access control list](#) and [Add IP entries](#).

- Enable access control for the listener. For more information, see [Enable access control](#).
- You can disable access control in the listener configuration. For more information, see [Disable access control](#).

2. Access control lists

2.1. Create an access control list

Before you configure access control for a listener, you must first configure an access control list.

Procedure

- 1.
- 2.
3. Select a region.
4. In the left-side navigation pane, click **Access Control**.
5. On the **Access Control** page, click **Create Access Control List**. In the panel that appears, enter a list name, select a resource group, and then select an IP version.
Enter multiple addresses in the following format:
 - Enter one entry per line. Press the Enter key to start a new line.
 - Use a vertical bar (|) to separate the IP address or CIDR block and the description within an entry.
Example: `192.168.1.0/24|Description`.
6. Click **Create**.

Related information

- [CreateAccessControlList](#)

2.2. Add IP entries

This topic describes how to add one or more IP entries to an access control list. An IP entry can be an IP address or a CIDR block.

Context

IP entries are the source IP addresses that are used to access the SLB instance. The features of access control lists vary based on the listener configurations.

- **Whitelist**: Only the requests from the IP addresses or CIDR blocks in the specified ACL are forwarded. You can use the whitelist feature when you want to allow access from specified IP addresses.
- **Blacklist**: Requests from the IP addresses or CIDR blocks in the specified ACL are not forwarded. You can use the blacklist feature when you want to deny access from specified IP addresses.

Procedure

- 1.
- 2.
3. Select a region.
4. In the left-side navigation pane, click **Access Control**.
5. Find the access control list to which you want to add IP entries and click **Manage** in the **Actions** column.
6. Add IP entries.

- On the Details page, click **Add Multiple Entries**. In the **Add Multiple IP Entries** panel, enter multiple IP addresses or CIDR blocks in the Add Multiple Addresses and Descriptions field, and click **Add**.

Enter multiple addresses in the following format:

- Enter one entry per line. Press the Enter key to start a new line.
 - Use a vertical bar (|) to separate the IP address or CIDR block and the description within an entry. Example: 192.168.1.0/24|Description.
- On the Details page, click **Add Entry**. In the **Add IP Entry** panel, enter an IP address or a CIDR block and a description. Then, click **Add**.

Related information

- [AddAccessControlListEntry](#)

2.3. Delete IP entries

This topic describes how to delete IP entries from an access control list.

Procedure

- 1.
- 2.
3. Select the target region.
4. In the left-side navigation pane, click **Access Control**.
5. Find the target access control list and click **Manage** in the **Actions** column.
6. Find the target IP entry and click **Delete** in the **Actions** column, or select multiple IP entries and click **Delete** at the bottom of the list.
7. In the dialog box that appears, click **OK**.

Related information

- [RemoveAccessControlListEntry](#)

3. Enable access control

This topic describes how to enable access control for a listener. You can enable access control for each listener of a Classic Load Balancer (CLB). You can set whitelists or blacklists for different listeners to regulate network access control.

Prerequisites

Before you enable access control, make sure that the following requirements are met:

- A network ACL is created. For more information, see [Create an access control list](#).
- A listener is created.

Procedure

- 1.
- 2.
3. Select the region where the CLB instance that you want to manage is created.
4. Click the ID of the CLB instance.
5. Click the **Listener** tab, find the listener that you want to manage, and then choose **⋮** > **Set Access Control** in the **Actions** column.
6. Set the following parameters and click **OK**.

Parameter	Description
Enable Access Control	Turn on the switch to enable access control for the listener.
Access Control Method	<p>Select an access control method. Valid values:</p> <ul style="list-style-type: none"> ◦ Whitelist: After you set a whitelist for a listener, the listener forwards only requests from IP addresses or CIDR blocks that are added to the whitelist. <p>However, your business may be adversely affected if the whitelist is not set properly. After you set a whitelist for a CLB listener, only requests from IP addresses or CIDR blocks that are added to the whitelist are distributed by the listener. After you enable the whitelist, if no IP address is added to the whitelist, the listener forwards all requests.</p> <ul style="list-style-type: none"> ◦ Blacklist: After you set a blacklist for a CLB listener, the listener blocks requests from IP addresses or CIDR blocks that are added to the blacklist. <p>After you enable a blacklist, if no IP address is added to the blacklist, the listener forwards all requests.</p>

Parameter	Description
Access Control List	<p>Select a network ACL.</p> <p>IPv6 instances can be associated only with IPv6 network ACLs, and IPv4 instances can be associated only with IPv4 network ACLs.</p> <div data-bbox="842 454 1385 636"><p> Note Separate multiple IP entries with commas (.). You can add up to 300 IP entries to each network ACL. IP entries must be unique within each network ACL.</p></div>

4. Disable access control

This topic describes how to disable access control for a listener.

Procedure

- 1.
2. Select a region.
3. Find an SLB instance and click its instance ID.
4. Click the **Listener** tab next to the **Instance Details** tab.
5. Find the listener for which you want to disable access control, and choose  > **Set Access Control** in the Actions column.
6. In the **Access Control Settings** panel, disable access control and then click OK.