Alibaba Cloud
Server Load Balancer

Access control

Issue: 20190725

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 informatio n, 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 Configure an access control list

Server Load Balancer (SLB) provides you with an access control function. You can configure different access control rules (whitelist or blacklist) for different listeners. Before configuring the access control function for a listener, you must first configure an access control list.

You can create multiple access control lists. Each list contains multiple IP addresses or CIDR blocks. Limits on access control lists are shown in the following table.

Resource	Limit
The maximum number of access control lists per region	50
The maximum number of IP entries added each time	50
The maximum number of IP entries per access control list	300
The maximum number of listeners with which an access control list can be associated	50

Create an access control list

To create an access control list, follow these steps:

1. Log on to the SLB console.
2. Select a region.
3. In the left-side navigation pane, click Access Control.
4. Click Create Access Control List, enter an access control list name, select the IP version, and select the resource group.
5. Click OK.

Add IP entries

To add IP entries to the access control list, follow these steps:

1. Log on to the SLB console.
2. Select a region.
3. In the left-side navigation pane, click Access Control.

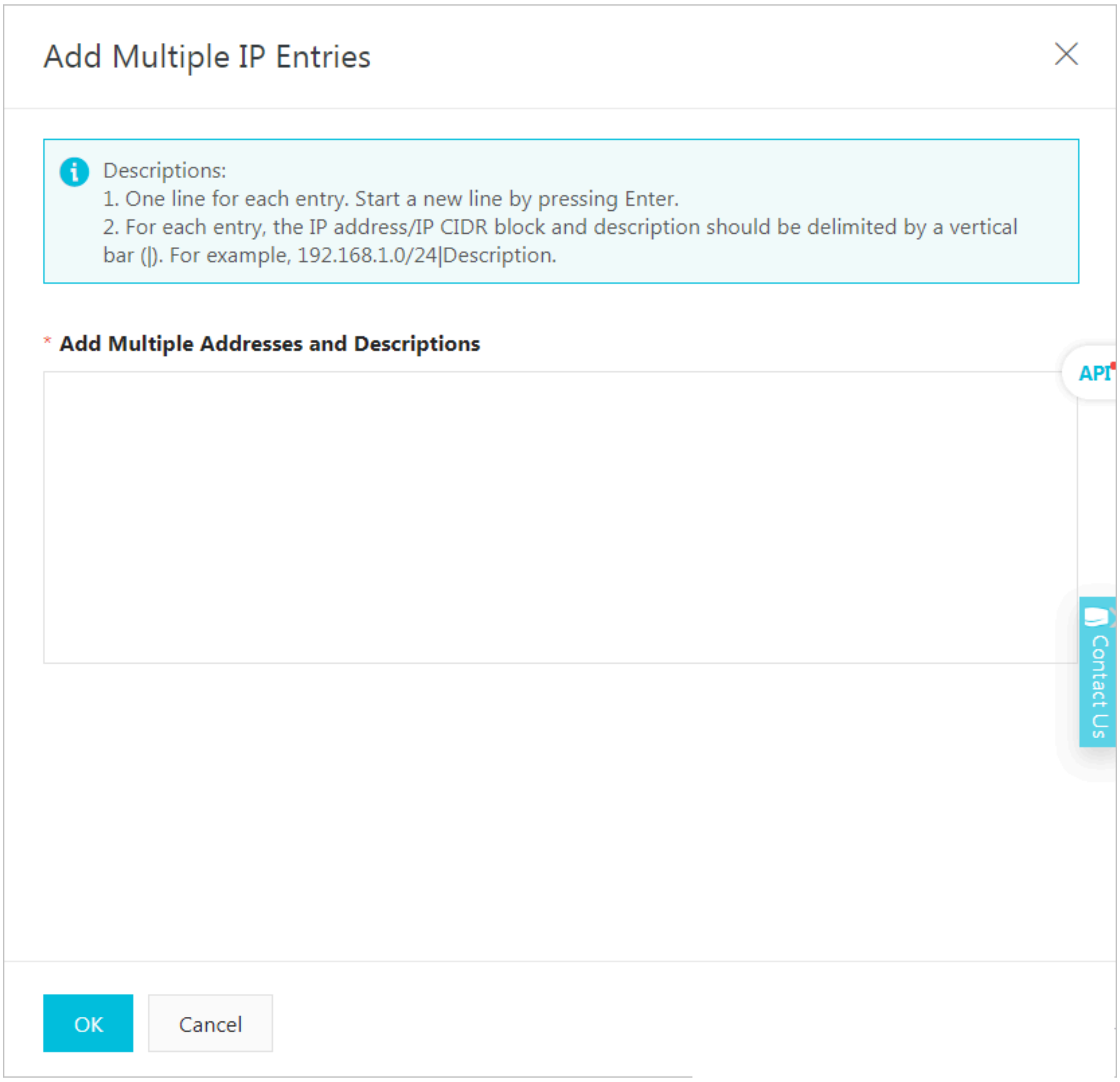
4. Find the target access control list and click Manage.

5. Add IP entries:

   - Click Add Multiple Entries. In the displayed dialog box, add IP addresses or CIDR blocks and click OK.

     Note the following when you add IP entries:

     - Each line should include only one IP entry. Use the Enter key to break lines.
     - Use a vertical bar (|) to separate an IP address or a CIDR block with the description, for example, 192.168.1.0/24|description.

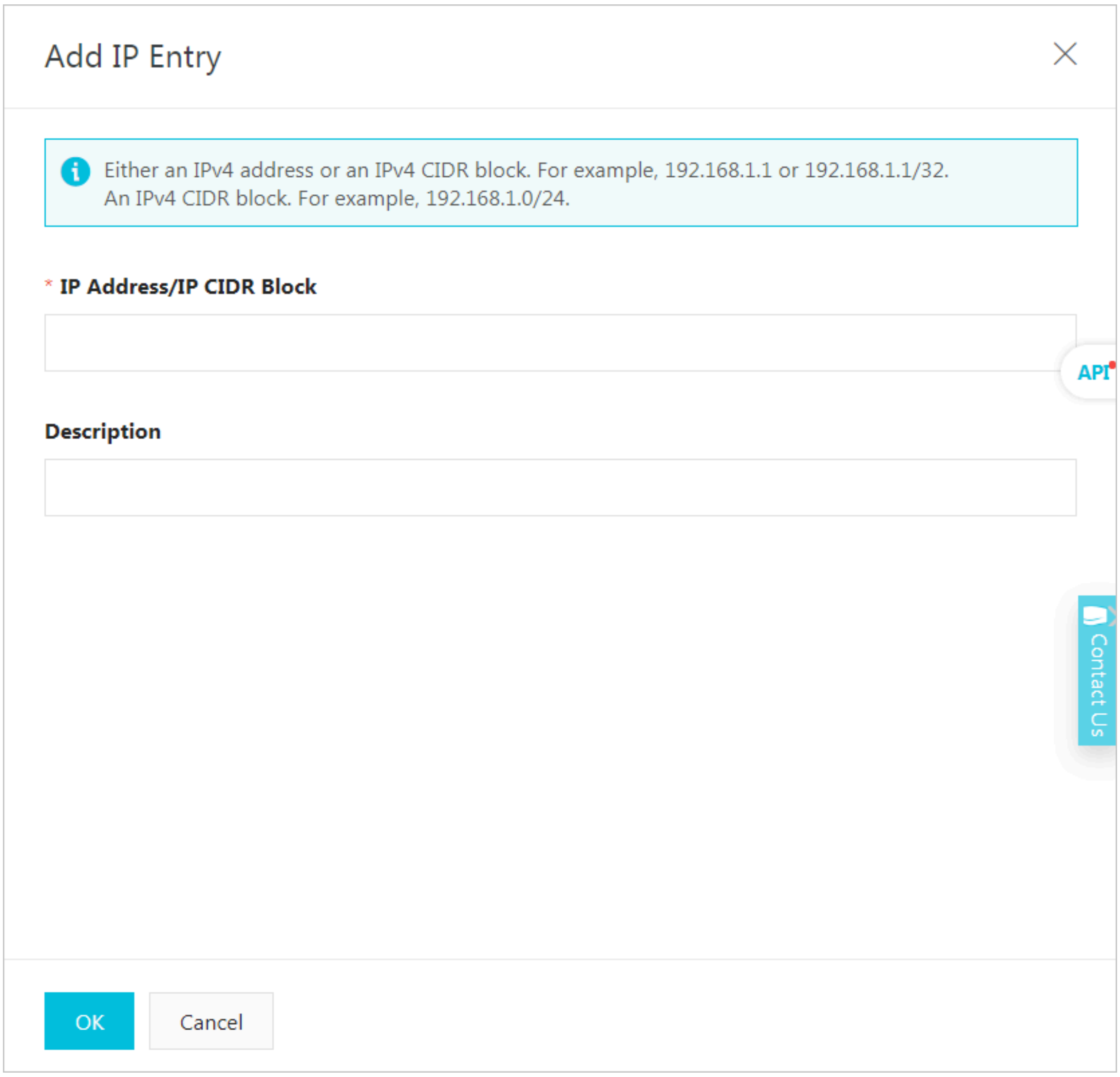
     

     Add Multiple IP Entries

     Descriptions:
     1. One line for each entry. Start a new line by pressing Enter.
     2. For each entry, the IP address/IP CIDR block and description should be delimited by a vertical bar (|). For example, 192.168.1.0/24|Description.

     * Add Multiple Addresses and Descriptions

   - Click Add Entry. In the displayed dialog box, add an IP address or a CIDR block and the description, and click OK.



Add IP Entry

Either an IPv4 address or an IPv4 CIDR block. For example, 192.168.1.1 or 192.168.1.1/32.
An IPv4 CIDR block. For example, 192.168.1.0/24.

* IP Address/IP CIDR Block

Description

Delete IP entries

To delete IP entries, follow these steps:

1. Log on to the SLB console.
2. Select a region.
3. In the left-side navigation pane, click Access Control.
4. Find the target access control list and click Manage.
5. Click Delete in the Actions column of the target IP entry, or select multiple IP entries and click Delete at the bottom of the list.
6. In the displayed dialog box, click OK.

2 Configure access control

Server Load Balancer (SLB) provides an access control function for listeners. You can configure different whitelists or blacklists for different listeners.

You can configure access control when you create a listener or change access control configurations after a listener is created.

This topic describes how to configure access control after a listener is created.

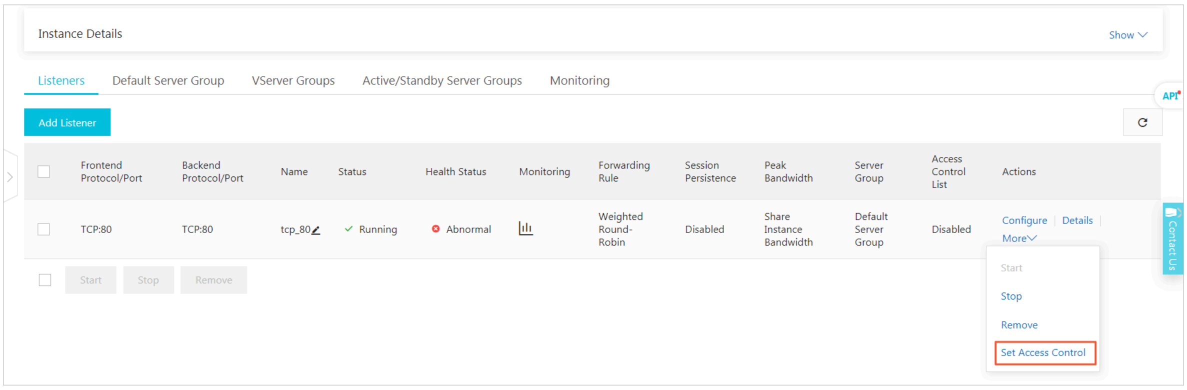
Enable access control

Before you enable access control, make sure:

- An access control list is created. For more information, see Configure an access control list.
- A listener is created.

To enable access control, follow these steps:

1. Log on to the SLB console.
2. Select the region of the target SLB instance.
3. Locate the target SLB instance and click the instance ID.
4. On the Instance Details page, click the Listeners tab.
5. Locate the target listener, and then choose More > Set Access Control.



□	Frontend Protocol/Port	Backend Protocol/Port	Name	Status	Health Status	Monitoring	Forwarding Rule	Session Persistence	Peak Bandwidth	Server Group	Access Control List	Actions
□	TCP:80	TCP:80	tcp_80	✓ Running	Abnormal		Weighted Round-Robin	Disabled	Share Instance Bandwidth	Default Server Group	Disabled	Configure | Details | More

6. On the Access Control Settings page, enable access control, select an access control method and an access control list, and click OK.

   - 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 business risks. 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, no 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.

Disable access control

To disable access control, follow these steps:

1. Log on to the SLB console.
2. Select the region of the target SLB instance.
3. Locate the target SLB instance and click the instance ID.
4. On the Instance Details page, click the Listeners tab.
5. Locate the target listener, and then click More > Set Access Control.
6. On the Access Control Settings page, disable access control and click OK.

3 Migrate to the new access control

If you have already configured a whitelist for a listener, Server Load Balancer can automatically add the IP addresses or CIDR blocks in the whitelist to an access control list and apply the list to the listener.

Migrate a whitelist to an access control list

To migrate a previously configured whitelist to an access control list, complete these steps:

1. Log on to the SLB console.
2. Select the region where the SLB instance is located, and then click the ID of the target SLB instance.
3. Click the Listeners tab.
4. Find the target listener, select More > Set Access Control.
5. Click Use New Access Control Features.
6. Enter a name of the access control list and click Create Access Control List.
7. Click Apply to apply the list to the listener as a whitelist.

> Note:
> If you do not apply the list to a listener, the whitelist does not take effect.

View the migrated access control list

To view the migrated access control list, complete these steps:

1. Log on to the SLB console.
2. Select a region.
3. In the left-side navigation pane, click Access Control.
4. Find the created access control list and view the associated listener. You can click Manage to manage IP entries.