Alibaba Cloud
Virtual Private Cloud

Access control

Issue: 20200527

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 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 contact Alibaba Cloud directly if you discover any errors in this document.

Document conventions

Style	Description	Example
	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.
	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.
	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.
	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 `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`

Style	Description	Example
{} or {a|b}	This format is used for a required value, where only one item can be selected.	switch {active|stand}

Contents

1 Overview

Virtual Private Cloud (VPC) allows you to create network access control lists (ACLs) to implement access control. In addition, it allows you to use access control features supported by other cloud services deployed in VPC networks to facilitate access control. For example, you can use security groups supported by Elastic Compute Service (ECS), or whitelists supported by Server Load Balancer (SLB) and ApsaraDB for RDS.

Network ACLs

Network ACL is a feature provided by VPC for network access control. You can customize the rules of a network ACL and associate the network ACL with a VSwitch to control inbound and outbound traffic of the ECS instances connected to the VSwitch. For more information, see #unique_4.

ECS security groups

Security groups act as virtual firewalls that provide Stateful Packet Inspection (SPI) and packet filtering features. Security groups are used to isolate security domains on the cloud. You can configure security group rules to control the inbound and outbound traffic of ECS instances in the group. For more information, see #unique_5.

RDS whitelists

To connect to an ApsaraDB for RDS instance that resides in a VPC, you must add the IP address of the client to the RDS whitelist. Otherwise, the client is unable to connect to the RDS instance. Requests from IP addresses that are not included in the whitelist are blocked. For more information, see #unique_6.

SLB whitelists

SLB is a service that distributes traffic to multiple ECS instances based on forwarding rules. You can configure IP addresses for SLB listeners to forward requests. This method is applicable when only specific IP addresses are allowed to access an application. For more information, see #unique_7.

2 Cases for configuring ECS security groups

When creating an ECS instance of the VPC network, you can either use the default security group or use other existing security groups in the VPC. A security group is a virtual firewall used to control the inbound and outbound traffic of an ECS instance.

This topic lists some common security group configurations for ECS instances of the VPC network.

Case 1: Intranet communication

The following are two types of communication methods between ECS instances of the VPC network:

- By default, ECS instances in the same security group of the same VPC can communicate with each other.
- ECS instances in different VPCs cannot communicate with each other. To achieve communication between two ECS instances in different VPCs, use Express Connect, VPN Gateway, or CEN to connect them. When doing so, make sure the security group rules allow access between the target ECS instances, as shown in the following table.

Security group rules	Rule direction	Authorization policy	Protocol type and port range	Authorization type	Authorization object
Security group configurations for the ECS instance in VPC 1	Inbound	Allow	Windows: RDP 3389/3389	Address field access	Enter the private IP address to access the ECS instance. To allow the access of any ECS instance, enter 0.0.0.0/0.
	Inbound	Allow	Linux: SSH 22/22	Address field access	
	Inbound	Allow	Custom TCP Custom	Address field access	

Security group rules	Rule direction	Authorization policy	Protocol type and port range	Authorization type	Authorization object
Security group configurations for the ECS instance in VPC 2	Inbound	Allow	Windows: RDP 3389/3389	Address field access	Enter the private IP address to access the ECS instance. To allow the access of any ECS instance, enter 0.0.0.0/0.
	Inbound	Allow	Linux: SSH 22/22	Address field access	
	Inbound	Allow	Custom TCP Custom	Address field access	

Case 2: Deny the access of specific IP addresses or ports

You can configure security groups to deny the access of specific IP addresses or ports to an ECS instance.

Security group rules	Rule direction	Authorization policy	Protocol type and port range	Authorization type	Authorization object
Deny the access of a specific IP address range to all ports of the ECS instance	Inbound	Drop	All -1	Address field access	Enter the IP address range to block, in the form of CIDR block, such as 10.0.0.1/32.
Deny the access of a specific IP address range to port 22 of the ECS instance	Inbound	Drop	SSH (22) 22/22	Address field access	Enter the IP address range to block, in the form of CIDR block, such as 10.0.0.1/32.

Case 3: Allow the remote access of a specific IP address

If you have configured a NAT Gateway or EIP for an ECS instance in a VPC, you can add the following security group rules to allow Windows remote logon or Linux SSH logon.

Security group rules	Rule direction	Authorization policy	Protocol type and port range	Authorization type	Authorization object
Allow Windows remote logon	Inbound	Allow	RDP 3389/3389	Address field access	To allow the logon of any public IP address, enter 0.0.0.0/0. To allow only the remote logon of a specific IP address, enter the IP address.
Allow Linux SSH logon	Inbound	Allow	SSH 22/22	Address field access	To allow the logon of any public IP address, enter 0.0.0.0/0. To allow only the remote logon of a specific IP address, enter the IP address.

Case 4: Allow access from the Internet to the HTTP/HTTPS service deployed on the ECS instance

If you have deployed a website on an ECS instance in a VPC and configured an EIP or NAT Gateway to provide services, configure the following security group rules to allow access from the Internet.

Security group rules	Rule direction	Authorization policy	Protocol type and port range	Authorization type	Authorization object
Allow access to port 80	Inbound	Allow	HTTP 80/80	Address field access	0.0.0.0/0
Allow access to port 443	Inbound	Allow	HTTPS 443/443	Address field access	0.0.0.0/0

Security group rules	Rule directi	Author ion policy	Protocol type and port range	Authoriza ion type	Authorization object
Allow access to port 80	Inbound	Allow	TCP 80/80	Address field access	0.0.0.0