

Virtual Private Cloud

Operation Guide

Product Documentation



Copyright Notice

©2013-2025 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by the Tencent corporate group, including its parent, subsidiaries and affiliated companies, as the case may be. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Operation Guide

Network Topology

Network performance dashboard

Virtual Private Cloud (VPC)

Overview

Limits

Creating VPC

Viewing VPCs

Editing IPv4 CIDR Blocks

Associating or Unassociating CCN

Modifying VPC DNS

Modifying VPC Name and Tag

Classiclink

Overview

Managing Classiclink

Enabling or Disabling Multicast

Deleting VPCs

Subnets

Creating Subnets

Viewing Subnet Information

Changing the Subnet Route Table

Managing ACL Rules

Enabling or Disabling Broadcast

Deleting a Subnet

Route Tables

Overview

Remarks

Creating Custom Route Tables

Associating or Disassociating Subnet

Managing Routing Policies

Deleting a Routing Table

IPs and ENIs

Elastic IP

HAVIPs

Overview

Limits

Managing HAVIP

Binding or Unbinding EIP

Querying HAVIPs

Releasing HAVIPs

ENIs

Bandwidth Package

Network Connection

NAT Gateway

VPN Connection

Direct Connect

Cloud Connect Network

Security Management

Security Groups

Overview

Creating a Security Group

Adding a Security Group Rule

Associating CVM Instances with Security Groups

Managing Security Groups

Viewing Security Groups

Removing Instances

Cloning a Security Group

Deleting a Security Group

Adjusting the Priorities of Security Groups

Managing Security Group Rules

Viewing a Security Group Rule

Modifying a Security Group Rule

Deleting a Security Group Rule

Importing a Security Group Rule

Exporting a Security Group Rule

Sorting Security Group Rules

Snapshot Rollback

Application Cases of Security Groups

Common Server Ports

Network ACL

Rule Overview

Limits

Managing Network ACLs

Parameter Template

- Overview

- Limits

- Managing Parameter Templates

- Configuration Case

Access Management

- Cloud Access Management Overview

- Authorizable Resource Types

- VPC Access Management Policy Examples

- Resource-Level Permissions Supported by VPC APIs

Diagnostic Tools

- Network Probe

- Instance Port Verification

- Flow Logs

- Traffic Mirroring

- Overview

- Use Limits

- Creating Traffic Mirror

- Managing Traffic Mirror

Snapshot Policy

- Overview

- Creating Snapshot Policy

- Associating, Disassociating, and Querying Security Group

- Enabling and Disabling Snapshot Policy

- Modifying Snapshot Policy

- Querying Snapshot Policy

- Deleting Snapshot Policy

Alarming and Monitoring

Operation Guide

Network Topology

Last updated : 2024-10-22 15:35:39

The network topology map displays all VPC resources, so that you can obtain VPC deployments and connections in real time.

Directions

1. Log in to the [VPC console](#).
2. Click **Network Topology Map** on the left sidebar.
3. Select a region and VPC to view cloud resources of the VPC such as CVM, CLB, TencentDB, and NoSQL, and their network topology relation.

Network performance dashboard

Last updated : 2024-10-22 15:36:18

The Network Performance Dashboard is designed to display the intra-region and inter-Availability Zone latency within supported Tencent Cloud regions, allowing you to stay informed about network performance and better plan your cloud resource distribution.

Instructions

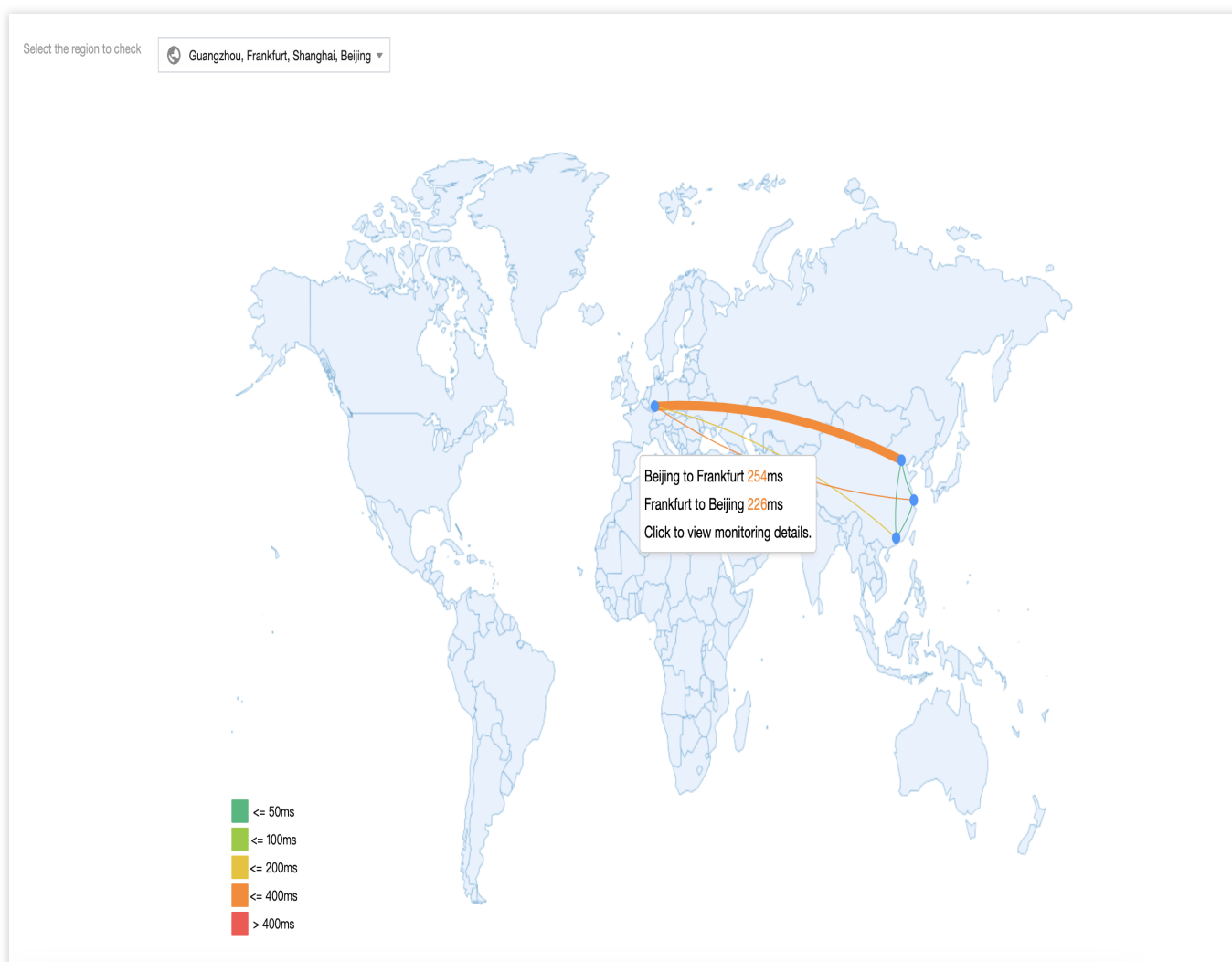
1. Log in to the [Virtual Private Cloud Console](#).
2. In the left sidebar, click **Network Performance Dashboard** to access the display interface.

Inter-region Intranet Performance

Note

The latency data before and after the exchange between the source and destination regions may vary due to differences in the underlying transmission lines.

Select a region and click on the inter-region connection line to view the network latency between the chosen regions.



Intra-region Intranet Performance

Select a region to view the network latency between Availability Zones within the region.



Note

No latency data is available for the same Availability Zone.

Virtual Private Cloud (VPC)

Overview

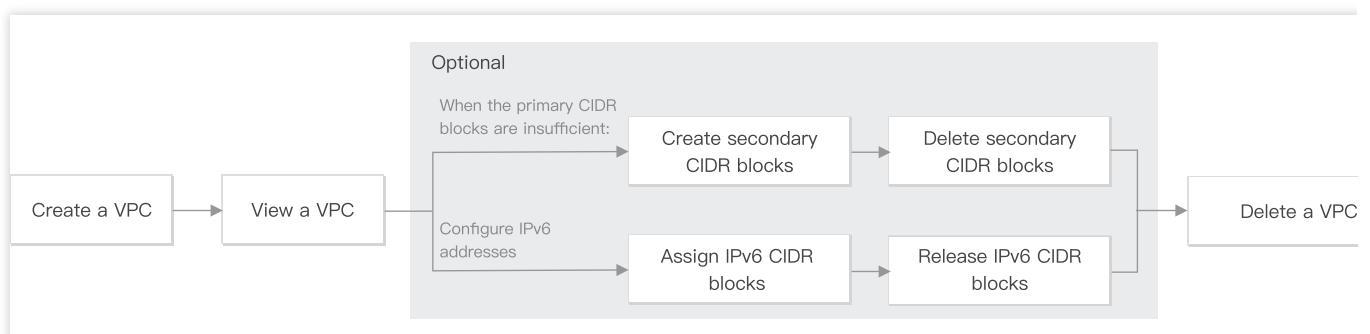
Last updated : 2024-10-22 15:36:36

A VPC is a logically isolated virtual network that you can use exclusively and plan independently on Tencent Cloud. To use any Tencent Cloud resource, you need to create a VPC and subnet. A subnet is a network space in the VPC. You can divide a VPC into at least one subnets. The VPC is regional, while the subnet is specific to the availability zone. Subnets in the same VPC can communicate with each other over a private network by default.

All cloud resources such as CVMs and CLBs in a VPC must be deployed in a subnet.

Lifecycle of VPC

The VPC lifecycle varies with needs, as shown below:



1. **Creating a VPC:** you need to carefully [plan your network](#) before creating a VPC. The CIDR blocks of VPCs and subnets cannot be modified after creation.
2. **Viewing a VPC:** you can view the basic information of a VPC, its CCN association, and the resources it contains.
3. (Optional) Choose the operations that apply to your use cases:
When the primary CIDR block is insufficient, see [Editing IPv4 CIDR Blocks](#):
[Creating secondary CIDR blocks](#): you can create secondary CIDR blocks to meet your actual network demands.
[Deleting secondary CIDR blocks](#): you can delete secondary CIDR blocks if you no longer need them.
4. **Deleting a VPC:** after a VPC is deleted, its subnets and route tables are also deleted.

Limits

Last updated : 2024-10-22 15:37:03

Use limits

The IP ranges of the VPC and subnet cannot be modified after creation.

For each subnet, Tencent Cloud reserves its first two IPs and the last one for IP networking. For example, if the [subnet CIDR block](#) is `172.16.0.0/24` , then `172.16.0.0` , `172.16.0.1` , and `172.16.0.255` are reserved by Tencent Cloud.

When you add a CVM to a VPC, the instance will be randomly assigned with a private IP from a specified subnet. You can reassign a private IP to it after the instance is created.

In a VPC, a CVM private IP corresponds to one public IP address.

Classic network-based CVMs cannot interconnect with cloud resources in the secondary CIDR block.

A peering connection does not support secondary CIDR blocks.

Cloud Connect Network, VPN gateway, and standard direct connect gateway support secondary CIDR blocks.

Quota limits

Resource	Limits
Number of VPC instances per region per account	20
Number of subnets per VPC	100
Number of secondary CIDR blocks per VPC	5

Note:

If you want to increase the quota, please [submit a ticket](#) to apply.

Creating VPC

Last updated : 2024-10-22 15:37:21

VPCs provide a basis for using Tencent Cloud services. This document describes how to create a VPC in the VPC console.

Operation Guide

1. Log in to the [VPC console](#).
2. Select a region at the top of the **VPC** page, and click **+ New**.
3. Enter the VPC information and subnet information in the **Create VPC** pop-up window.

Note:

The CIDR blocks of the VPC and subnet cannot be modified after creation.

The VPC CIDR block can be any of the following IP ranges. For VPCs to communicate with each other over a private network, their CIDR blocks should not overlap.

10.0.0.0 - 10.255.255.255 (mask range required to be between 12 and 28)

172.16.0.0 - 172.31.255.255 (mask range between 12 and 28)

192.168.0.0 - 192.168.255.255 (mask range between 16 and 28)

The subnet CIDR block must fall within or be the same as the VPC CIDR block.

For example, if the VPC IP range is 10.0.0.0/16 , then its subnet IP range can be 10.0.0.0/16 ,

10.0.0.0/24 , etc.

Availability zone: a subnet is specific to an availability zone. Select an availability zone in which the subnet resides. A VPC allows for subnets in different availability zone and by default these subnets can communicate with each other via a private network.

Associated route table: the subnet must be associated with a route table for traffic forwarding. A default route table will be associated to ensure private network interconnection in the VPC.

Tags: You can optionally add tags to help you better manage resource permissions of sub-users and collaborators.

Create VPC

VPC information

Region

South China(Guangzhou)

Name

Up to 60 characters ([a-z], [A-Z], [0-9] and [-_]).

IPv4 CIDR Block

10

.

0

.

0.0

/

16

The IP range cannot be changed once created. It's recommended to have a proper [network structure](#).

Tags

Tag key

Tag value

+ Add

Subnet information

Subnet name

Up to 60 characters ([a-z], [A-Z], [0-9] and [-_]).

IPv4 CIDR Block

10.0.

0

.

0

/

24

Remaining IPs: 253

Availability zone

Please select

Associated route table

Default

Tags

Tag key


Tag value

+ Add

OK





Close

4. After completing the configurations, click **OK**. A successfully created VPC will be displayed in the list, as shown below. A new VPC has a subnet and a default route table.

VPC 






Help of V

[+ New](#)

ID/Name	IPv4 CIDR Block 	Subnet	Route Table	NAT Gateway	VPN Gateway	CVM	Direct Conn...	Default VPC	Creation Time	Operation
vpc- 	10.0.0.0/16	1	1	0	0	0 	0	No	2021-07-05 12:18:47	Delete More 

Related Operations

After the VPC and subnet have been created, you can deploy resources including CVM and CLB within the VPC. Click the icon as shown below to directly purchase a CVM on the CVM purchase page. For more information, see [Building Up an IPv4 VPC](#).




ID/Name	IPv4 CIDR Block 	Subnet	Route Table	NAT Gateway	VPN Gateway	CVM	Direct Conn...	Default VPC	Creation Time	Operation
vpc- 	172. 	1	1	0	0	1 	0	No	2021-07-02 12:03:41	Delete More 

Related Content

There is a default VPC; that is:

When purchasing an instance such as CVM, CLB or TencentDB, you can choose to automatically create a default VPC and subnet without manual creation, as shown below:

Availability Zone Random AZ Chengdu Zone 1 Chengdu Zone 2

Network vpc- | Default-VPC (Default) | subnet- | Default-Subnet (Defa |  Available IPs in the subnet: 4089

The current network is the default VPC/subnet. You can adjust it as needed.

If the existing VPC/subnet do not match your requirements, please go to the Console to [Create a VPC](#) or [Create Subnet](#). You can change the VPC and subnet later in the console.

The default VPC and subnet are created together with your instance, and do not count against your quota in the region. They work the same as the manually-created ones. There can only be a single default VPC in a given region and a single default subnet in a given availability zone. You can delete the default VPC and subnet if you no longer need them.

VPC

Help of VPC

+ New

Please enter the VPC

ID/Name	IPv4 CIDR Block	Subnet	Route Table	NAT Gateway	VPN Gateway	CVM	Direct Conn...	Default VPC	Creation Time	Operation
vpc- Default-VPC		1	1	0	0	3	0	Yes	2020-05-08 14:44:39	Delete More

Subnet

All VPCs

Help of Subnet

+ New

Filter

Separate keywords with "|"; press Enter to separate filter

ID/Name	Network	CIDR	Availability Z...	Associated ro...	CVM	Available IPs	Default Subnet	Creation Time	Operation
subnet Default-Subnet	vpc- Default-VPC	10.202.0.0/20	w Zone 1	rtb- default	3	4088	Yes	2021-06-24 19:21:41	Delete More

Viewing VPCs

Last updated : 2024-10-22 15:37:45

You can query all VPC resources via the VPC console, such as cloud resources and connections in a VPC.

Directions

1. Log in to the [VPC console](#).
2. Select the region of the VPC at the top of the **VPC** page. You can check the information of all VPC in this region in the list.

Column	Description
ID/Name	The ID and name of the VPC. The name can be modified.
IPv4 CIDR Block	The IPv4 CIDR block of the VPC. It cannot be modified.
IPv6 CIDR block	The IPv6 CIDR block of the VPC. This feature is currently in beta. To use it, please submit a ticket .
Subnet	The number of subnets in the VPC. Click the number to access the Subnet page.
Route Table	The number of route tables in the VPC. Click the number to access the Route Table page.
NAT Gateway	The number of NAT Gateways in the VPC. Click the number to access the NAT Gateway page.
VPN Gateway	The number of VPN gateways in the VPC. Click the number to access the VPN Gateway page.
CVM	The number of CVMs in the VPC. Click the number to access the CVM page. Click the CVM icon to redirect to the CVM purchase page.
Direct Connect Gateway	The number of direct connect gateways in the VPC. Click the number to access the Direct Connect Gateway page.
Default VPC	Indicates whether the VPC is the default VPC of the region. There can only be one default VPC in a region. The default VPC is automatically created when you purchase resources like CVM. It works the same as the manually-created ones.
Creation Time	The time when the VPC was created.
Operation	The supported operations of the VPC. Only a VPC without any resource can be

deleted. You can click More to edit IPv4 CIDR block and IPv6 CIDR block if applicable.

3. Click the VPC ID to view details, including the basic information, CCN association, and associated resources. Click the number next to a resource to access the resource management page.
4. Return to the VPC list, and click in the top-right corner search box to filter VPC by different resource attributes.
5. Click the setting icon in the upper-right corner to customize display columns.

Editing IPv4 CIDR Blocks

Last updated : 2024-10-22 15:38:01

Each VPC can have one primary CIDR block, which cannot be modified after the VPC creation. When the IPs in the primary CIDR block can not meet your needs, you can create multiple secondary CIDR blocks to add IP ranges. You can allocate the subnet with an IP range from the primary or secondary CIDR blocks. All subnets of the same VPC are interconnected by default, regardless of whether they belong to the primary or secondary CIDR blocks.

Use Limits

Classic network-based CVMs cannot interconnect with cloud resources in the secondary CIDR block.

A peering connection does not support secondary CIDR blocks.

Cloud Connect Network, VPN gateway, and standard direct connect gateway supports secondary CIDR blocks. Note the following limits for a direct connect gateway:

This feature is unavailable in the Finance Cloud regions.

Up to 10 secondary CIDR blocks can be propagated.

This feature is unavailable to a NAT direct connect gateway.

Creating Secondary CIDR Blocks

1. Log in to the [VPC console](#).
2. Select the region of the VPC at the top of the **VPC** page.
3. In the VPC list, locate the VPC and select **More > Edit IPv4 CIDR block** under the **Operation** column.
4. In the pop-up dialog box, click **Add** to enter a secondary CIDR block.

Note:

A secondary CIDR block can overlap with the destination IP range of a custom route. Note that the secondary CIDR block uses a local route, which has a higher priority than that of custom subnet routes.

5. Click **OK**.

Deleting Secondary CIDR Blocks

1. Log in to the [VPC console](#).
2. Select the region of the VPC at the top of the **VPC** page.
3. In the VPC list, locate the VPC from which secondary CIDR blocks will be deleted, and select **More > Edit IPv4 CIDR block** under the **Operation** column.

4. In the pop-up dialog box, click **Delete** next to the secondary CIDR block.
5. Click **OK**.

Associating or Unassociating CCN

Last updated : 2024-10-22 15:38:18

Cloud Connect Network (CCN) bridges Tencent Cloud VPCs and between VPCs and local IDCs. It provides you with multipoint private network interconnection. To leverage this CCN feature, you need first to add VPCs to a CCN. This document describes how to associate a VPC with or disassociate it from a CCN.

Associating with CCN

1. Log in to the [VPC console](#).
2. Select the region of the VPC at the top of the **VPC** page.
3. Click the VPC ID to access the **Basic Information** page.
4. Click **Associate Now** under **Associate with CCN** to open the **Associate with CCN** dialog box.
5. Configure parameters as follows.

Account: the account of the CCN instance owner. The VPC and CCN instance can be under the same or different accounts. If you choose **Other accounts**, enter the **Account ID**. The account owner needs to accept the CCN application within 7 days, otherwise the application will expire. The owner of the CCN assumes the network interconnection fee generated by instances connecting to the CCN.

CCN ID: select a CCN ID from the drop-down list for **My Account** or enter a CCN ID for **Other accounts**.

6. Click **OK**. Then the status will be **Connected** as shown below.

Disassociating from CCN

1. Log in to the [VPC console](#).
2. Select the region of the VPC at the top of the **VPC** page.
3. Locate the VPC to disassociate from the CCN, and click the VPC ID to access the **Basic Information** page.
4. Click **Disassociate** in the **Associate with CCN** section.
5. Double check and confirm the operation risks and click **Disassociate**.

Relevant Operations

[Network Instance Interconnection in One Account](#)

[Network Instance Interconnection Crossing Account](#)

Modifying VPC DNS

Last updated : 2024-10-22 15:38:39

CVMs in a Tencent Cloud VPC support DHCP. The configurable DHCP options include DNS address and domain name. This document describes how to modify the DNS address and domain name of a VPC.

Note:

Dynamic Host Configuration Protocol (DHCP) is a LAN network protocol that defines the standard for transferring configuration information to TCP/IP network servers.

For now, VPCs created before April 1, 2018 do not support DHCP features. If you cannot modify the DNS address and domain name in the console, it means that your VPC does not support these features.

Notes

The new configurations will take effect on all CVMs in the VPC.

For newly created CVMs, the modified configurations take effect immediately.

For existing CVMs, the modified configurations take effect after the CVMs or network services are restarted.

Directions

1. Log in to the [VPC console](#).
2. Select the region of the VPC at the top of the **VPC** page.
3. Click the VPC ID to access the **Basic Information** page.
4. Click the edit icon to modify DNS and domain name respectively.

DNS: DNS server addresses

Note:

The Tencent Cloud default DNS is “183.60.83.19” and “183.60.82.98”. If the default DNS is not used, internal services such as Windows activation, NTP, and YUM will be unavailable.

DNS supports a maximum of four IP addresses. Separate IPs with commas. Note that certain operating systems might be unable to support four DNS addresses.

Domain Name: CVM hostname suffix, such as “example.com”. You can enter up to 60 characters, or keep the default configuration if you don’t have special requirements.

Details of vpc-

Basic Information

Classiclink

Basic Information

IPv4 CIDR

DNS ⓘ

Domain Name ⓘ

Tag

None

Modifying VPC Name and Tag

Last updated : 2024-10-22 15:38:58

This document describes how to modify the name, tag or other information of a VPC.

Directions

1. Log in to the [VPC console](#).
2. Select the region of the VPC at the top of the **VPC** page.
3. Click the edit icon next to a VPC name to modify it.
4. Click the VPC ID to access the **Basic Information** page.
5. Tags are used to identify and manage resources. You can click the edit icon to add or delete tags.

Classiclink

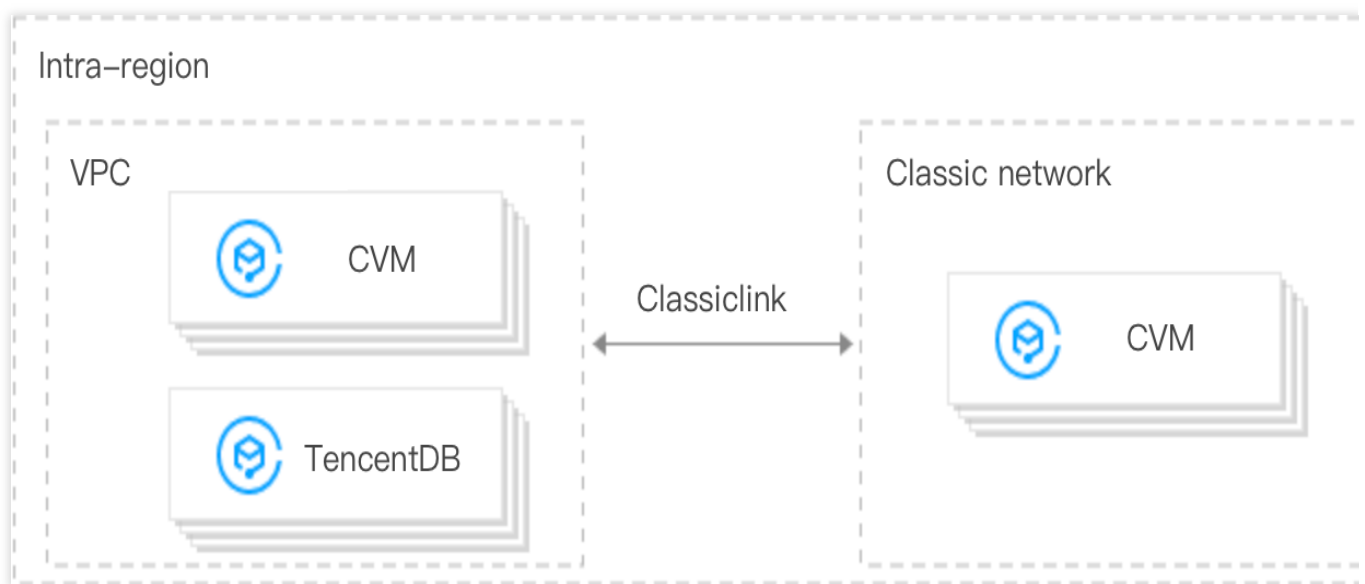
Overview

Last updated : 2024-10-22 15:39:15

The Classiclink feature allows VPC-based resources to communicate with classic network-based CVMs. For example,

The classic network-based CVMs can communicate with VPC resources such as CVM, TencentDB, private network CLB, Redis/CMEM, etc.

VPC resources can only access classic network-based CVMs, but not other resources in the classic network, like TencentDB and CLB



Use Limits

A VPC can only be interconnected with the classic network **in the same region**.

The VPC IP range must be within `10.0.0.0/16-10.47.0.0/16` (including subsets), otherwise there may be IP conflicts, which may cause failure while associating and communicating with the classic network-based CVMs.

A classic network-based CVM can only be associated with one VPC at a time.

One VPC supports associating with up to 100 classic network-based CVMs.

After the classic network-based CVMs are associated with a VPC, classic network-based CVMs can only communicate with resources in primary CIDR block rather than secondary CIDR block of the VPC.

CLB instances within a VPC cannot be bound to a classic network-based CVM that interconnects with the same VPC.

In Classiclink situations, the CVM traffic can only be routed to private IP addresses within the VPC rather than destinations outside the VPC.

Note:

The classic network-based CVM cannot access the public or private network resources outside the current VPC through network devices such as VPN gateway, direct connect gateway, public gateway, peering connection, and NAT Gateway. Likewise, the peer of a VPN gateway, direct connect gateway, and peering connection cannot access classic network-based CVMs.

Notes

Changing the private IP of a classic network-based CVM will invalidate its association with the VPC, and cause the configurations to become invalid. To associate them, you need to add a Classiclink again on the VPC console. The Classiclink will not be affected by actions taken regarding the CVM such as isolation due to overdue payment, security isolation, cold migration, failover, configuration modification, and operating system switching. The CVM will be automatically disassociated from the VPC if the CVM is returned.

Reference

For more information on Classiclink, see [Managing Classiclink](#).

Managing Classiclink

Last updated : 2024-10-22 15:39:59

Creating a Classiclink

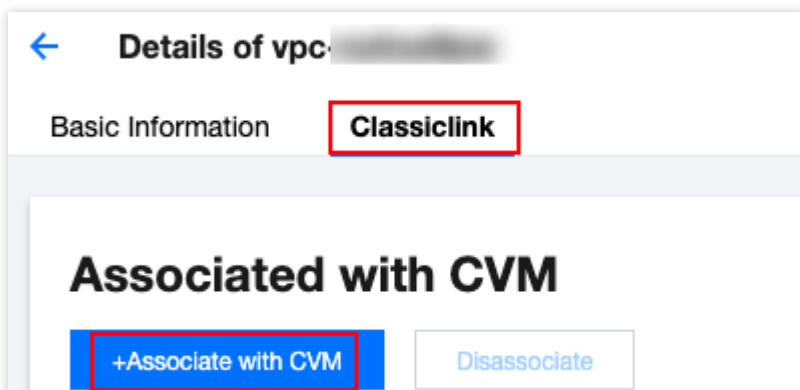
A Classiclink associates classic network-based CVMs with a VPC to enable interconnection between the VPC and the classic network. This allows classic network-based CVMs to communicate with VPC resources.

Note:

The private IPs of the associated classic network-based CVMs will be automatically added to the local policy of the VPC's route table. This allows interconnection, without the need to manually modify the routing policy of the VPC. After the classic network-based CVM is associated with a VPC, their firewall and network ACL settings will remain effective.

Directions

1. Log in to the [VPC console](#).
2. Select the region, and click the ID of the VPC which needs Classiclink to access the details page.
3. Click the **Classiclink** tab and then click **+Associate with CVM**.



4. In the pop-up window, select the CVM in the classic network to be associated with the VPC and click **OK**.

Associate with CVM

Select a CVM

0 selected

☐ 未命名
ins-XXXXXXXXXX

No data yet

↔

OK

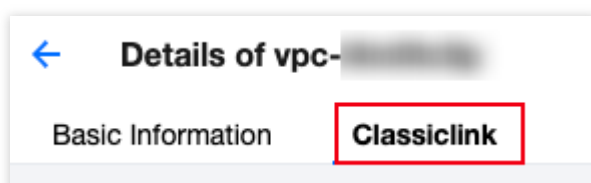
Close

Viewing Classiclink

You can view the list of classic network-based CVMs that interconnect with the VPC.

Directions

1. Log in to the [VPC console](#).
2. Select the region, and click the ID of the VPC which needs Classiclink to access the details page.
3. Click the **Classiclink** tab to view the list of classic network-based CVMs associated with the VPC.



4. Enter a private IP in the top-right corner search box to quickly locate the CVM.

Deleting a Classiclink

This action disassociates classic network-based CVMs from the VPC and terminates their interconnection.

Directions

1. Log in to the [VPC console](#).
2. Click the ID of the VPC which needs Classiclink to access the details page.
3. Click the **Classiclink** tab, select the CVM to be disassociated from the list of classic network-based CVMs, and click **Disassociate** in the **Operation** column.

The screenshot shows the 'Details of vpc-' page in the Tencent Cloud console. The 'Classiclink' tab is selected. Under 'Associated with CVM', there are buttons for '+Associate with CVM' and 'Disassociate'. A search bar 'Search by private IP' is also present. Below is a table with columns: CVM ID, Name, Private IP, and Operation. One CVM is listed with ID 'ins-', Name '未命名', and Private IP '10.'. The 'Disassociate' button in the Operation column is highlighted with a red box. A confirmation dialog is displayed over the table, asking 'Are you sure you want to disassociate with this classic network CVM?' and stating 'After being disassociated, this CVM will not be able to access this VPC.' with 'OK' and 'Cancel' buttons.

CVM ID	Name	Private IP	Operation
ins-	未命名	10.	Disassociate

4. Double check the notes and click **OK**.
5. To disassociate multiple CVMs, you can select these CVMs to be disassociated and click **Disassociate** above the list.

Enabling or Disabling Multicast

Last updated : 2024-10-22 15:40:14

This document describes how to enable or disable multicast for VPCs.

Background

Broadcast and multicast are modes of one-to-many communication, which can save businesses on the network bandwidth and reduce network load through point-to-multipoint efficient data transmission.

In the unicast mode, the initiating server sends data to N servers separately. If the multicast mode, the server sends the same data to N servers in once, which reduces the server resource consumption and also the bandwidth resource of the backbone network.

Note:

The trial period has ended. Please stay tuned for the official launch.

Multicast and broadcast are available in Beijing, Shanghai, Guangzhou, Chengdu, Chongqing, Nanjing, Hong Kong, Singapore, Seoul, Tokyo, Bangkok, Silicon Valley, Virginia and Frankfurt.

For single-VPC multicast and broadcast, up to 50,000 PPS and 190 Mbps are supported.

Multicast: Tencent Cloud supports multicast on the VPC dimension.

Broadcast: Tencent Cloud supports broadcast on the subnet dimension.

Overview

Multicast and broadcast are mostly used in the financial and game industries:

Broadcast services or market data of the financial industry. For example, after obtaining stock prices and other real-time data, brokers can broadcast stock data to multiple clients in real time, effectively reducing network load.

For the game industry, broadcast and multicast are mainly used for heartbeat holding between multiple servers.

How It Works

Enabling multicast

1. Log in to the [VPC console](#).
2. In the VPC list, locate the target VPC, and toggle on **Multicast**.

Disabling multicast

1. Log in to the [VPC console](#).
2. In the VPC list, locate the target VPC, and toggle off **Multicast**.

More

For detailed directions regarding the subnet broadcast, see [Enabling/Disabling Broadcast](#).

Deleting VPCs

Last updated : 2024-10-22 15:40:30

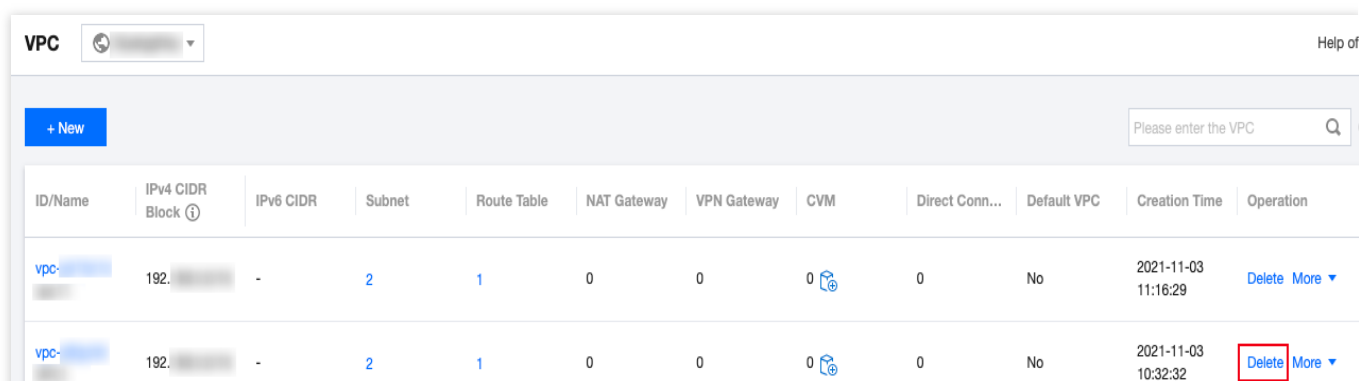
When a VPC is no longer in use and has no other resources (Peering Connections, ClassicLink, NAT Gateway, VPN Gateway, Direct Connect Gateway, CCN, and private connection) except empty subnets, routing tables, and network ACLs, it can be deleted.

Note:

An empty subnet refers to a subnet that does not use any IPs; that is, when there are only empty subnets, routing tables, and network ACLs in a VPC, the VPC can be deleted; when there is IP use in a subnet, the VPC cannot be deleted.

Directions

1. Log in to the [VPC console](#).
2. Select the region of the VPC at the top of the **VPC** page.
3. In the VPC list, locate the VPC to delete, click **Delete** in the **Operation** column, and confirm the deletion.



VPC Help of											
<div><div>+ New</div><div>Please enter the VPC Q</div></div>											
ID/Name	IPv4 CIDR Block ⓘ	IPv6 CIDR	Subnet	Route Table	NAT Gateway	VPN Gateway	CVM	Direct Conn...	Default VPC	Creation Time	Operation
vpc- [redacted]	192. [redacted]	-	2	1	0	0	0	0	No	2021-11-03 11:16:29	Delete More ▼
vpc- [redacted]	192. [redacted]	-	2	1	0	0	0	0	No	2021-11-03 10:32:32	Delete More ▼

Subnets

Creating Subnets

Last updated : 2024-10-22 15:40:54

A subnet is a network space in a VPC, which carries all the cloud resource deployments. A VPC has at least one subnet. A subnet will be created together with the VPC. You can also create more subnets in a VPC according to your business needs.

A subnet is specific to an availability zone. A VPC allows subnets in different availability zones, and these subnets can communicate with each other via a private network by default. This document guides you through how to create a subnet in a VPC.

Directions

1. Log in to the [VPC console](#).
2. Click **Subnet** on the left sidebar to access the management page.
3. Select the region and VPC in which the subnet will be created and click **+New**.
4. Configure the subnet parameters in the pop-up dialog box.

Create a Subnet

Network vpc- | 10.1 ▾ 1 existing subnets

Subnet Name	VPC IP Range	CIDR ⓘ	Availability Zone ⓘ	Associated route table ⓘ	Operation
<input type="text" value="Enter the subnet name"/> 0/60	▾	10 . 11 . <input type="text" value="64"/> . 0 / <input type="text" value="24"/> ▾	Guangzhou Zone 1 ▾	default ▾	-
+Add a line					
Advanced Options ▸					

Create Cancel

Network: the VPC where the subnet resides. The VPC selected in [step 3](#) will be automatically displayed. Alternatively, you can select a VPC from the drop-down list.

Subnet Name: enter a custom subnet name within 60 characters.

VPC IP Range: the CIDR block of the selected VPC will be automatically displayed.

CIDR: set the CIDR block of the subnet, which must be part of the VPC CIDR block and cannot overlap with the CIDR block of other existing subnets under the VPC.

Note:

Plan subnet IP ranges that suit your business scale. A private IP address within the specified subnet will be automatically assigned to the CVM instance you are creating. The primary private IP of a CVM can be modified. For more information, see [Modifying Primary Private IP](#).

Availability Zone: select an availability zone where the subnet resides.

Associated route table: select a route table to be associated. The subnet must be associated with a route table to control outbound traffic. The default route table of the VPC will be associated by default to ensure private network interconnection in the VPC. You can also select another route table within the VPC.

Add a line: click **Add a line** to create multiple subnets at a time. Click



to delete the selected subnet settings.

Advanced Options: you can optionally set tags for the subnet to better manage subnet resources. Click **Add** to set multiple tags at a time. You can click the icon in the **Operation** column to delete the selected tag settings.

5. After completing the configurations, click **Create**. Then subnets that have been successfully created will be displayed in the list, as shown below.

Subnet Guangzhou All VPCs Help of Subnet										
+ New Filter		Separate keywords with " "; press Enter to separate filter Q								
ID/Name	Network	CIDR	IPv6 CIDR	Availability ...	Associated...	CVM	Available IPs	Default Sub...	Creation Ti...	Operation
subnet- [redacted]	vpc- [redacted]	[redacted]	-	Guangzhou Zone 4	rtb- def	0	251	No	2021-06-11 10:37:52	Delete More
subnet- [redacted]	vpc- [redacted]	[redacted]	-	Guangzhou Zone 1	rtb-7	0	29	No	2021-06-01 14:59:41	Delete More

Subsequent Operation

After creating a subnet, you can deploy resources including CVM and CLB in it.

Click the icon as shown below to directly purchase a CVM on the CVM purchase page. For more information, see [Building Up an IPv4 VPC](#).

ID/Name	IPv4 CIDR Block	Subnet	Route Table	NAT Gateway	VPN Gateway	CVM	Direct Conn...	Default VPC	Creation Time	Operation
vpc- VPC	/16	1	1	0	0	0	0	No	2021-02-03 22:01:11	Delete More

Viewing Subnet Information

Last updated : 2024-10-22 15:41:17

You can view the resources of all subnets in the VPC on the VPC console, for instance, the cloud resources deployed in the subnet, the route table associated with the subnet, and the ACL rules bound to the subnet.

How It Works

1. Log in to the [VPC console](#).
2. Click **Subnet** on the left sidebar to access the subnet management page.
3. At the top of the **Subnet** page, select the region and VPC to which the subnet belongs. If you keep the default value, namely **All VPCs**, then you can view all subnets of all VPCs in this region.

Note

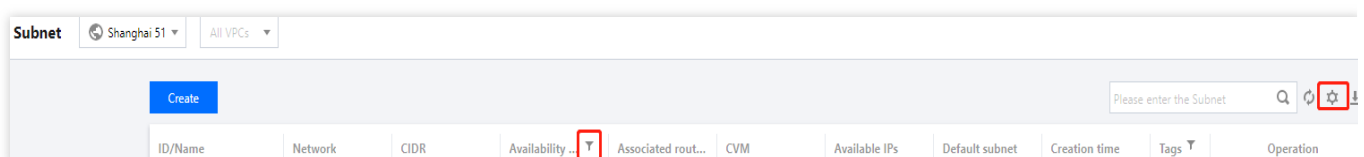
Click the VPC ID of the network to which the subnet belongs, or the route table ID of the associated route table to view the detailed information of the corresponding resource.

Click the number of CVMs to go to the CVM instance page. If the quantity is 0, click the CVM icon to go to the CVM purchase page.

Click the Filter icon next to the **Availability zone** field and select an availability zone to view all subnets in the availability zone.

Click the search box in the top-right of the list to query subnets by **Subnet ID**, **Subnet Name**, **Tag**, **Keyword** and **IPv4 CIDR Block**.

Click the Setting icon in the upper right to customize the displayed fields.



The meaning of the list fields displayed in the interface is as follows:

ID/Name: The subnet ID and name. Each subnet is assigned an ID when it is created, and the subnet name can be modified on your own.

Network: The VPC to which the subnet belongs.

CIDR: The CIDR block of the subnet. It cannot be modified once confirmed.

Availability Zone: The availability zone where the subnet is located.

Associated Route Table: The route table associated with the subnet.

CVM: Number of CVMs deployed in the subnet.

Available IPs: Number of available IP addresses within the CIDR block of the subnet.

Default subnet: Default subnets are subnets created automatically by Tencent Cloud upon the launch of new CVM instances. Each region has one and only default VPC and subnet.

Creation Time: The subnet creation time.

Tags: You can optionally add tags to help you better manage resource permissions of sub-users and collaborators.

Operation: Available actions. A subnet can be deleted when it's not associated with any resource. Click **More >**

Change Route Table to replace the route table associated with the subnet.

4. Click the subnet ID to view the resource details of the subnet. Switch the tab to view the routing rules and the ACL rules.

Basic information

Routing rules

ACL rules

Basic information

Subnet name

Subnet ID

Subnet CIDR block

Network

Region

Shanghai

Availability zone

Shanghai Zone 4


Associate ACL

You've not configured the ACL. [Bind](#)

Default subnet

No

Tags

No tags found 

Creation time

2023-01-12 04:37:57

Changing the Subnet Route Table

Last updated : 2024-10-22 15:41:40

Each subnet must be associated with one [route table](#), which is used to control the outbound traffic direction of the subnet. You can change the Subnet's associated route table in the **VPC -> Subnet** page according to the routing needs of the subnet. If you need to create a route table, please see [Creating a Custom Route Table](#).

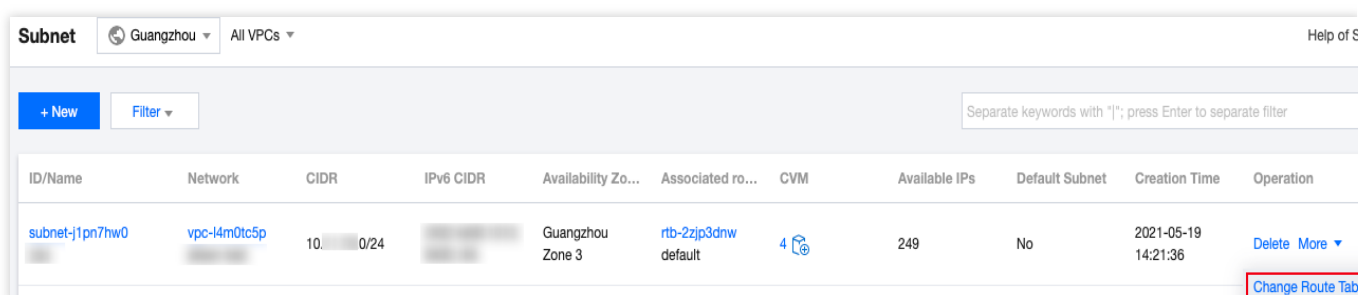
Systems impact

Considering that the route table directly impacts the traffic flow in the subnet, any changes such as route table association or route entries must be carefully considered in accordance to the business needs of the network flows.

Directions

1. Log in to the [VPC console](#).
2. Select **Subnet** in the left sidebar to go to the subnet management page.
3. The system provides two methods to change the route table associated with the subnet.

Click **More > Change Route Table** in the **Operation** column on the right side of the subnet that needs to change the route table.



ID/Name	Network	CIDR	IPv6 CIDR	Availability Zo...	Associated ro...	CVM	Available IPs	Default Subnet	Creation Time	Operation
subnet-j1pn7hw0	vpc-l4m0tc5p	10.0.0/24		Guangzhou Zone 3	rtb-2zjp3dnw default	4	249	No	2021-05-19 14:21:36	Delete More

Click the ID of the subnet that needs to change the route table to go to the details page, switch to the **Routing Rules** tab, and click **Change Route Table**.

Details of subnet [redacted] Help of St

Basic Information **Routing Rules** ACL Rules

Routing Rules

Bound route table default (rtb-[redacted]) [Change Route Table](#)


Destination	Next hop type	Next hop	Notes
10. [redacted] /18	LOCAL	Local Local	Delivered by default, indicates that CVMs in the VPC

4. In the pop-up window, select a new route table in the drop-down list, confirm the impact on your business, and click **Confirm**.

Change Route Table ×

Change Route Table

default ▼

 After the change, the new route table policies will be applied to associated instances immediately. Please make sure your business will not be affected by this change.

Confirm

Cancel

Managing ACL Rules

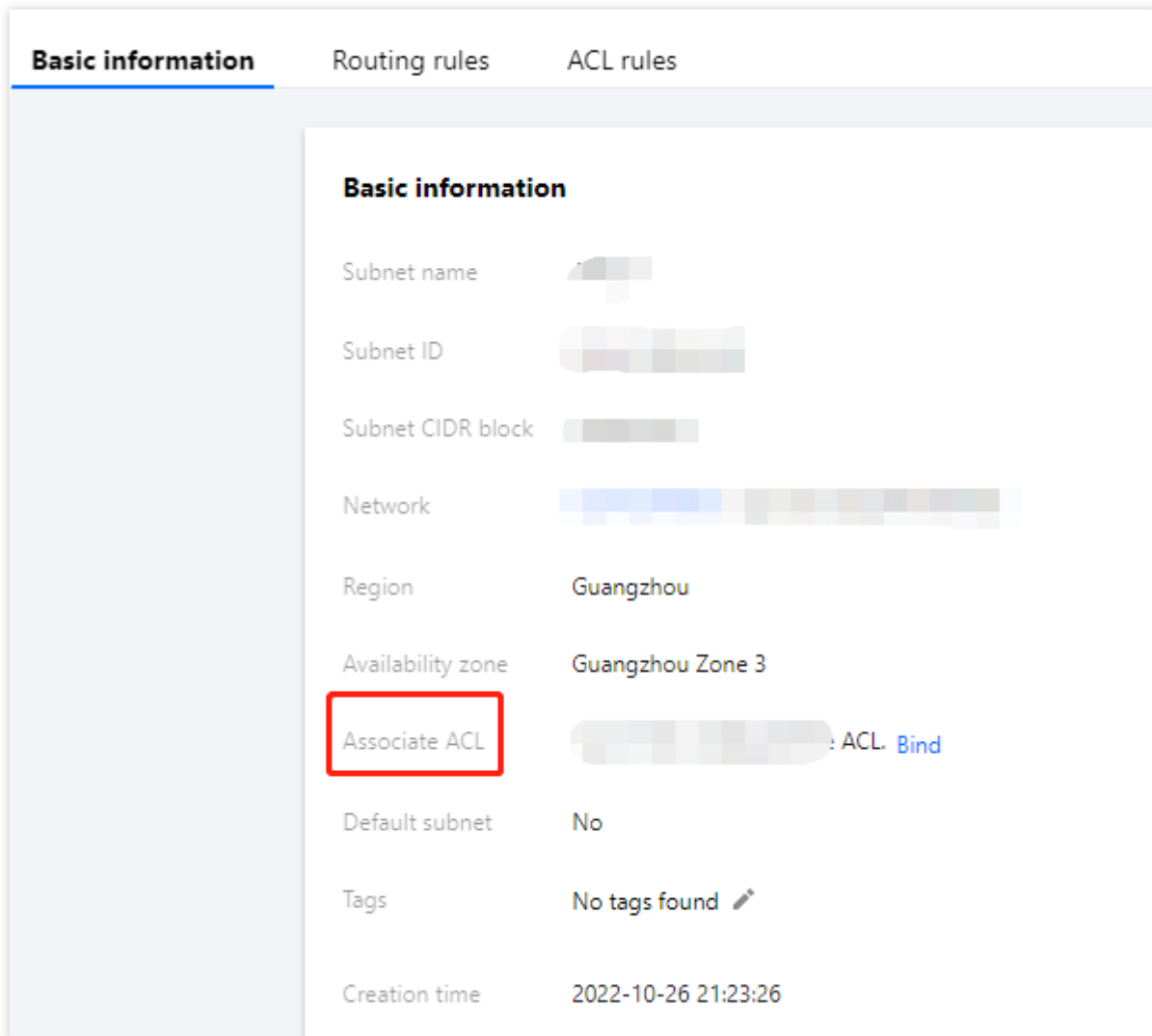
Last updated : 2024-10-22 15:41:59

The [ACL Rule](#) is an optional security layer which operates at subnet level. It is used to control the inbound and outbound data streams of subnets, which can be accurate to the protocol and port granularity, to achieve fine-control of subnet traffic. You can associate the same network ACL to subnets which require the same level of network traffic control.

This document describes how to bind, unbind, and change ACL rules in the VPC console.

How It Works

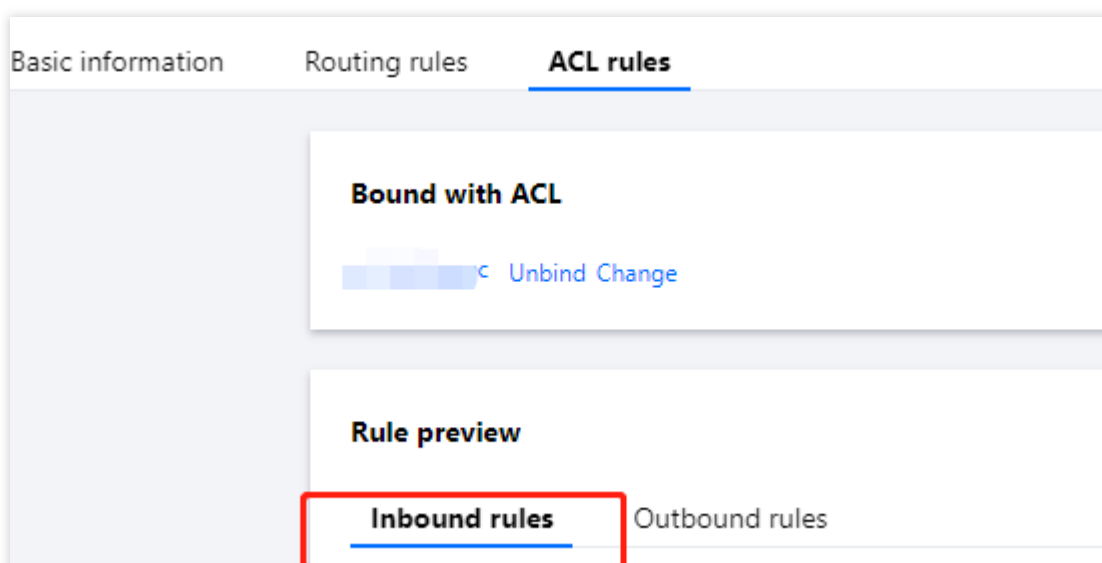
1. Log in to the [VPC console](#).
2. Click **Subnet** on the left sidebar to access the subnet management page.
3. Click a subnet ID to go to its details page. You can bind, unbind, and change ACL rules on the following tabs:
In the **Associate ACL** field under the **Basic information** tab



The screenshot displays the 'Basic information' tab of a subnet configuration page. The page has three tabs: 'Basic information', 'Routing rules', and 'ACL rules'. The 'Basic information' tab is active. It shows various details about the subnet, including its name, ID, CIDR block, network, region (Guangzhou), and availability zone (Guangzhou Zone 3). A red box highlights the 'Associate ACL' button, which is currently disabled. Other buttons like 'Bind' are visible. The 'Default subnet' is set to 'No', and there are 'No tags found'. The creation time is '2022-10-26 21:23:26'.

Field	Value
Subnet name	[Redacted]
Subnet ID	[Redacted]
Subnet CIDR block	[Redacted]
Network	[Redacted]
Region	Guangzhou
Availability zone	Guangzhou Zone 3
Associate ACL	[Redacted] ACL. Bind
Default subnet	No
Tags	No tags found
Creation time	2022-10-26 21:23:26

Under the **ACL rules** tab

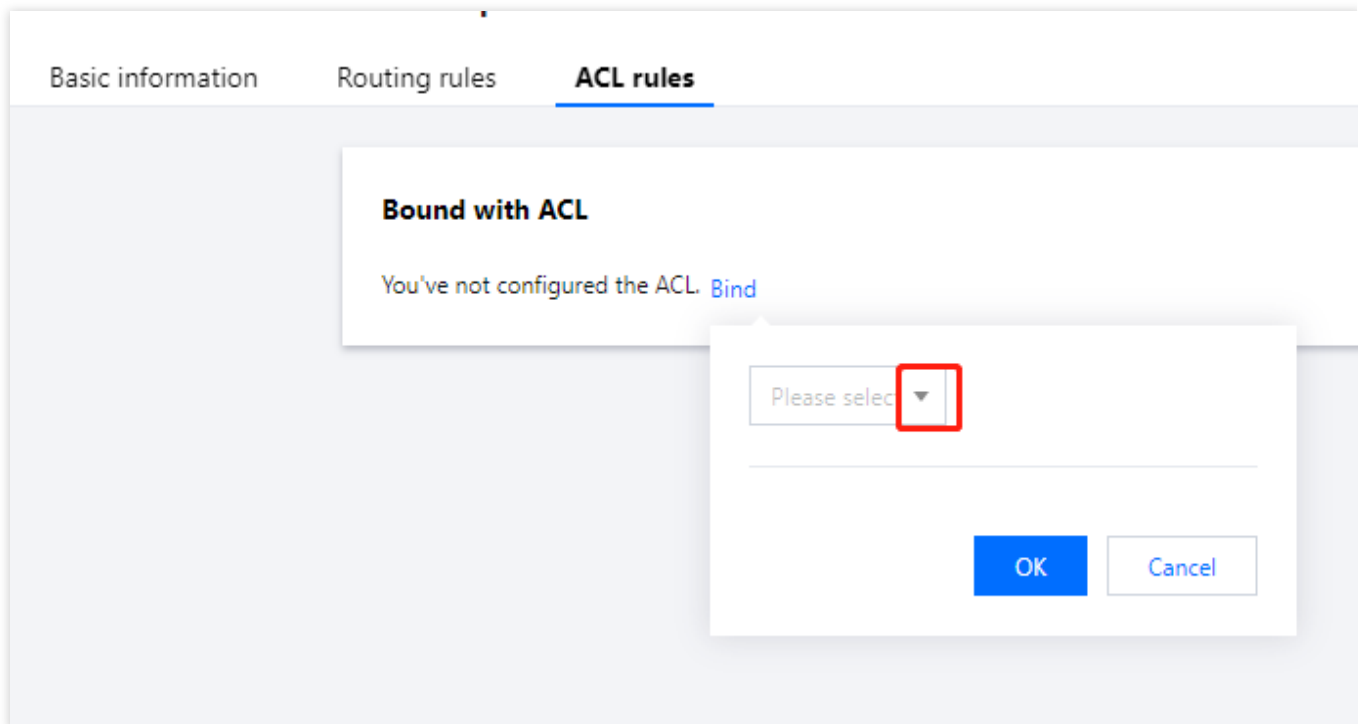


The screenshot displays the 'ACL rules' tab of the subnet configuration page. It shows a 'Bound with ACL' section with a button to 'Unbind Change'. Below this is a 'Rule preview' section with two tabs: 'Inbound rules' (highlighted with a red box) and 'Outbound rules'.

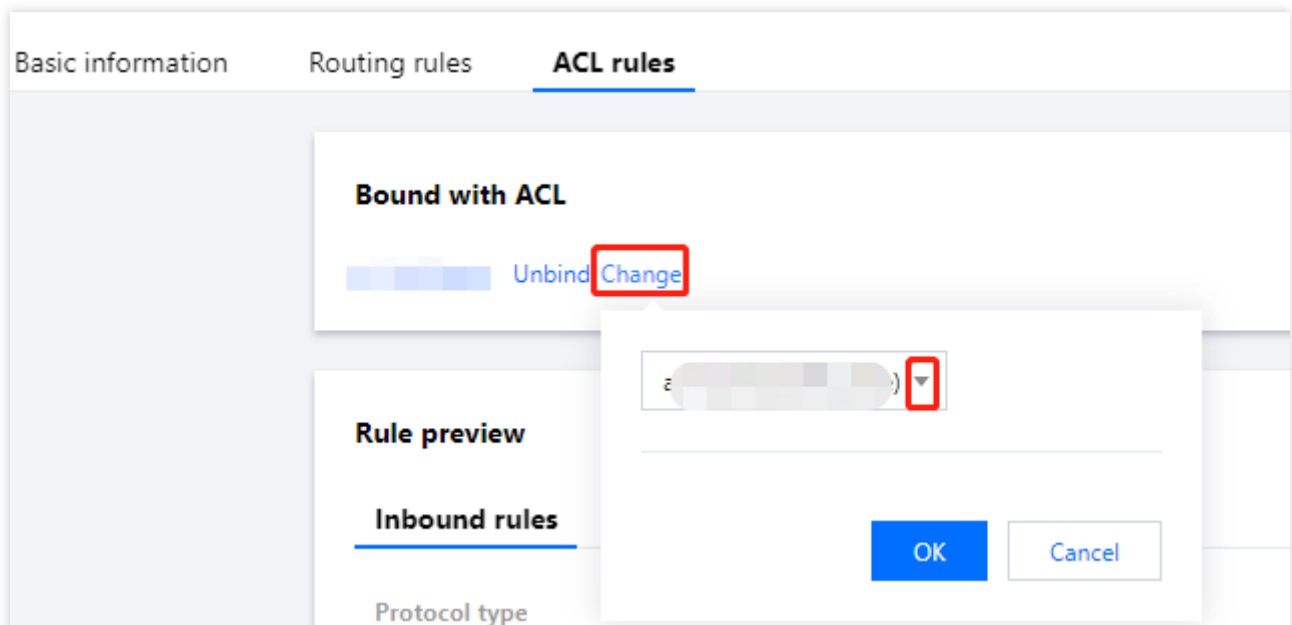
Section	Content
Bound with ACL	[Redacted] Unbind Change
Rule preview	Inbound rules (selected), Outbound rules

4. Perform the following operations based on the business needs. The following screenshots take the operations in **ACL Rules** as an example.

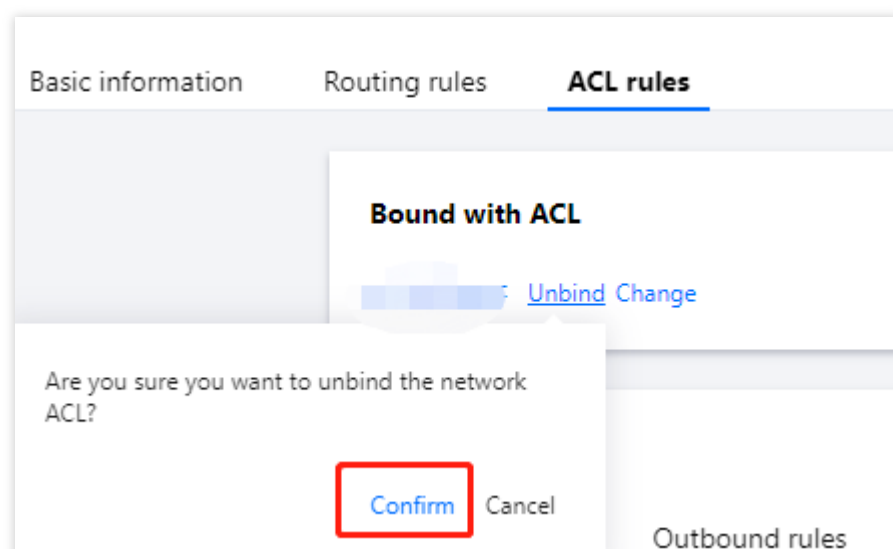
If the current subnet is not bound to an ACL rule, you can click **Bind** to select an appropriate ACL rule, and click **OK** to complete the binding. The binding will take effect immediately. The inbound and outbound traffic of the subnet is allowed only when the rule is **Allow**.



If the ACL rule bound to the current subnet does not meet network flow requirements, you can click **Change** to change the ACL rule, which will take effect immediately.



If the current subnet is bound to an ACL rule, but you no longer need to control the inbound and outbound traffic of the subnet, you can click **Unbind** to unbind the ACL rule. The unbinding will take effect immediately and this will cause the lifting of the ACL rule restriction on the inbound and outbound traffic of the subnet.



Enabling or Disabling Broadcast

Last updated : 2024-10-22 15:42:38

Background

Broadcast and multicast are modes of one-to-many communication, which can save businesses on the network bandwidth and reduce network load through point-to-multipoint efficient data transmission.

In the unicast mode, the initiating server sends data to N servers separately. If the multicast mode, the server sends the same data to N servers in once, which reduces the server resource consumption and also the bandwidth resource of the backbone network.

Multicast: Tencent Cloud supports multicast on the VPC dimension.

Broadcast: Tencent Cloud supports broadcast on the subnet dimension.

Note:

The trail period of VPC has

Multicast and broadcast are available in Beijing, Shanghai, Guangzhou, Chengdu, Chongqing, Nanjing, Hong Kong, Singapore, Seoul, Tokyo, Bangkok, Silicon Valley, Virginia and Frankfurt.

For single-VPC multicast and broadcast, up to 50,000 PPS and 190 Mbps are supported.

Scenarios

Multicast and broadcast are mostly used in the financial and game industries:

Broadcast services or market data of the financial industry. For example, after obtaining stock prices and other real-time data, brokers can broadcast stock data to multiple clients in real time, effectively reducing network load.

For the game industry, broadcast and multicast are mainly used for heartbeat holding between multiple servers.

Directions

Enabling broadcast

1. Log in to the [VPC console](#).
2. Click **Subnet** on the left sidebar.
3. In the VPC list page, locate the target VPC, and toggle on **Subnet broadcast**.

Disabling broadcast

1. Log in to the [VPC console](#).

2. Click **Subnet** on the left sidebar.
3. In the VPC list page, locate the target VPC, and toggle off **Subnet broadcast**.

Related Operations

For information about VPC-level multicast, see [Enabling/Disabling Multicast](#).

Deleting a Subnet

Last updated : 2024-10-22 15:42:57

You can delete the subnets that are no longer in use and do not use any IP resources.

Note:

Currently, Tencent Cloud resources that involve IP use in subnets include CVM, private network CLB, ENI, HAVIP, SCF, TKE, and TencentDB (for MySQL, Redis, TDSQL, etc.).

Directions

1. Log in to the [VPC console](#).
2. Click **Subnet** on the left sidebar to access the management page.
3. At the top of the list, select the region and VPC that the subnet to be deleted belongs to.
4. In the list, select the subnet to delete, click **Delete** in the **Operation** column, and click **OK**.

Subnet										
Guangzhou		All VPCs		Help of S						
+ New		Filter		Separate keywords with " "; press Enter to separate filter						
ID/Name	Network	CIDR	IPv6 CIDR	Availability Zo...	Associated ro...	CVM	Available IPs	Default Subnet	Creation Time	Operation
subnet-j1pn7hw0	vpc-l4m0tc5p	10. /24		Guangzhou Zone 3	rtb-2zjp3dnw	4	249	No	2021-05-19 14:21:36	Delete More

Route Tables

Overview

Last updated : 2024-10-22 15:44:14

A route table consists of multiple routing policies that control the outbound traffic direction of subnets in the VPC. Each subnet can only be associated with one route table, while each route table can be associated with multiple subnets. You can create multiple route tables for subnets with different traffic routes.

Types

There are two types of route tables: default and custom.

Default route table: When you create a VPC, the system automatically generates a default route table, which will be associated with subnets created later if no custom route table is selected. You cannot delete the default route table, but you can add, delete, and modify routing policies in it.

Custom route table: You can create or delete a custom route table in the VPC. This custom route table can be associated with all the subnets to apply the same routing policy.

Note:

You can associate a route table when [creating a subnet](#), or [changing the route table](#) after a subnet is created.

Routing Policy

A route table controls traffic routes by using routing policies. A routing policy consists of the destination, next-hop type, and next hop:

Destination: Specifies the destination IP range to which you want to forward the traffic. It should be an IP range. If you want to enter a single IP address, set the mask to `32` (for example, `172.16.1.1/32`). The destination cannot be an IP range of the VPC where the route table resides, because the local route already allows private network interconnection in this VPC.

Note:

If you have [Tencent Kubernetes Engine](#) deployed in your VPC, when you create a route table policy for the VPC subnet, the destination range cannot be within the VPC IP range or the [container IP range](#).

If the container network and VPC routes overlap, traffic will be preferentially forwarded within the container network.

Next-hop type: Indicates the egress of data packets for the VPC. The next-hop type of VPC supports **NAT Gateway**, **Peering connection**, **VPN Gateway**, **Direct Connect gateway**, **CVM**, and others.

Next hop: Specifies the next hop instance (identified by the next-hop ID) to which the traffic is forwarded, such as a NAT gateway in the VPC.

Routing policy priority

When there are multiple routing policies in a route table, the following routing priority applies, from high to low:

Traffic within the VPC: Traffic within the VPC is matched first.

Exact match route (the longest prefix match): When there are multiple routes in the route table that can match the destination IP, the route with the longest (exact) mask is matched to determine the next hop.

Public IP: If no routing policy is matched, a CVM instance can access the internet through its public IP address.

Use case:

When a subnet is associated with a NAT gateway, and the CVM instance in the subnet has a public IP (or EIP), the CVM instance accesses the internet through the NAT gateway by default (because the priority of the exact match route is higher than that of the public IP). However, you can set a routing policy to allow the CVM instance to access the internet through its public IP address. For more information, see [Adjusting the Priorities of NAT Gateways and EIPs](#).

ECMP

Equal-cost multipath (ECMP) routing means there are multiple equal-cost routes to a single destination. The traditional routing technology only uses one path to transfer packets to the same destination, while the remaining paths are in the standby or invalid status. When the path fails, it takes time to switch to another path. By contrast, ECMP uses multiple equal-cost routes in the network environment to increase the transfer bandwidth, balance traffic over multiple routes, and achieve backup with redundant linkages.

ECMP with VPC routes of the same type is as detailed below:

Next hop type	Whether ECMP Is Formed with Routes of the Same Type	Maximum Number of Routes Supported by ECMP
NAT Gateway	Yes	N/A
CVM public IP	No	N/A
CVM	Yes	Up to eight routes of the same type
Peering connection	No	N/A
Direct Connect gateway	No	N/A
CCN	No	N/A
HAVIP	Yes	Up to eight routes of the same type
VPN Gateway	Yes	Up to eight routes of the same type

ECMP with VPC routes of different types is as detailed below:

NAT gateways and CVM instances can form the ECMP.

If there is already a self-learning CCN route, when a configured custom route to a Direct Connect gateway/peering connection is added, CCN and the Direct Connect gateway/peering connection can form the ECMP.

If there is already a custom route for the Direct Connect gateway/peering connection, and you want to form the ECMP with CCN, [submit a ticket](#) for assistance.

Use cases

ECMP is often used to balance the traffic load over gateways with a limited bandwidth. Assume that you need 2,000 Mbps to interconnect your VPC-based and IDC-based businesses, but the current maximum VPN bandwidth is 1,000 Mbps. To achieve the goal, you can create two 1,000-Mbps VPN gateways and two VPN tunnels.

Primary/Secondary Routes

Primary and secondary routes refer to two or more paths to the same destination with only one active path. Assume there are two VPC routes to the IDC, that is, paths A and B. All packets are sent to the destination via path A, while path B is invalid or on standby. When path A suffers linkage failures, you can switch to path B to take over traffic from path A, thus ensuring business availability. In this case, paths A and B are called primary and secondary routes.

The next hop type determines the route priority. When adding a routing policy to the VPC route table, you can configure different types of gateways to act as primary and secondary routes to a single destination. Then, the VPC network probe can be used to check the linkage quality and accessibility. After configuring an alarm policy, you can promptly detect any linkage exception and quickly switch between primary and secondary routes to meet the high availability requirements.

Note:

VPC does not have the route priority feature by default. This feature is currently in beta test. To try it out, [submit a ticket](#) for application.

The next hop type determines the route priority in the VPC route table. By default, the route priority from high to low is CCN, Direct Connect gateway, VPN Gateway, and others.

Currently, you cannot adjust the route priority in the console. If needed, [submit a ticket](#) for assistance.

The following table describes the primary/secondary support of different types of VPC routes:

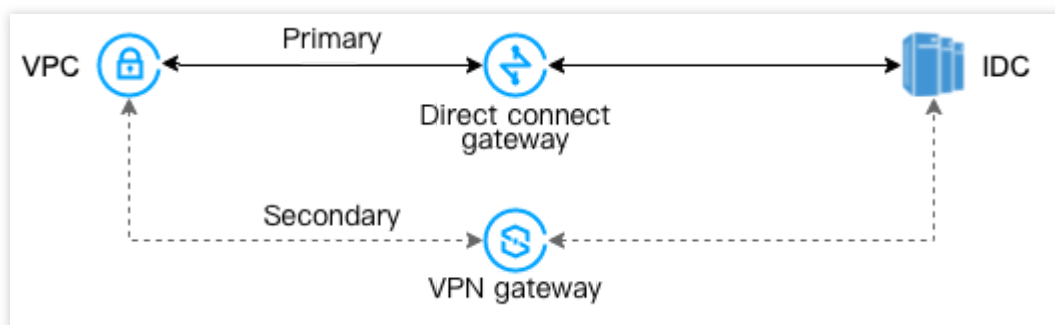
Next Hop Type	Support for Primary/Secondary Routes
NAT Gateway	No
Public IP of CVM	No
CVM	Yes, with CCN, VPN Gateway, Direct Connect gateway, or HAVIP
Peering connection (intra-region)	No

Peering connection (cross-region)	No
Direct Connect gateway	Yes, with CCN, VPN Gateway, HAVIP, or CVM
CCN	Yes, with VPN Gateway, Direct Connect gateway, HAVIP, or CVM
HAVIP	Yes, with CCN, VPN Gateway, Direct Connect gateway, or CVM
VPN Gateway	Yes, with CCN, Direct Connect gateway, HAVIP, or CVM

Use cases

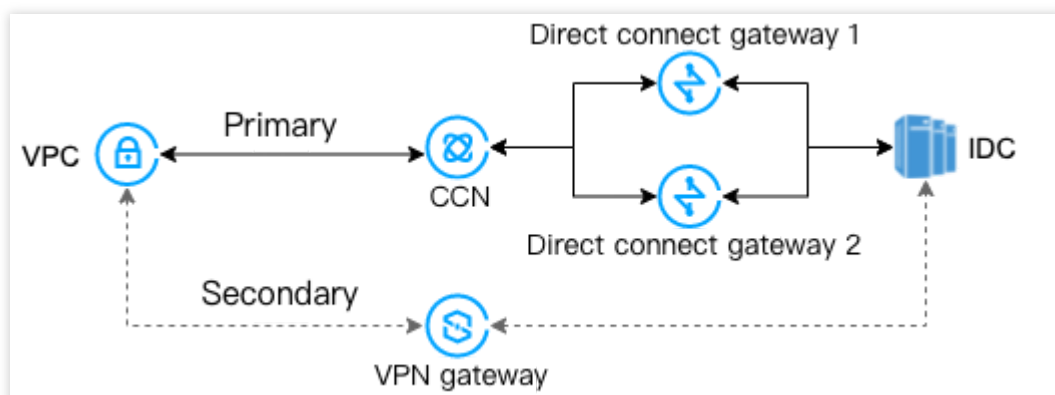
Primary and secondary routes are often used to smoothly forward traffic when a gateway linkage fails, for example: VPC-based Direct Connect gateway (primary) and VPN gateway for VPC (secondary)

Scenario: Interconnect a Tencent Cloud VPC and an on-premises IDC through a VPC-based Direct Connect gateway. Meanwhile, create VPN tunnels through a VPN gateway to act as the secondary communication linkage between the IDC and VPC.



CCN-based Direct Connect gateway (primary) and VPN gateway for VPC (secondary)

Scenario: Interconnect a Tencent Cloud VPC and an on-premises IDC through a CCN instance. Meanwhile, create VPN tunnels through a VPN gateway to act as the secondary communication linkage between the IDC and VPC.



Remarks

Last updated : 2024-10-22 15:44:35

The default route table of a VPC cannot be deleted.

After a VPC is created, its route table will be automatically provided with a default route, indicating that all resources in this VPC are interconnected through the private network. This routing policy cannot be modified or deleted.

Destination	Next hop type	Next hop
Local	Local	Local

Dynamic routing protocols such as BGP and OSPF are not supported.

Routes can be published to CCN. The following routes can be published to CCN.

Next hop type	Publishing to CCN by default	Manually publishing or withdrawing	Description
Local	Supported	Not supported	Assigned by the system. The VPC IP range connecting to CCN will be automatically published to CCN, including primary and secondary CIDR blocks (except for TKE IP ranges).
CVM	Not supported	Supported	A custom route to CVM. When the IP range is all 0 or the routing policy is disabled, the route cannot be published to CCN.
HAVIP	Not supported	Supported	Custom route to HAVIP. When the IP range is all 0 or the routing policy is disabled, the routes cannot be published to CCN.

Note:

A disabled custom route cannot be published to CCN.

A custom route should be withdrawn first before it can be disabled if it has been published to a CCN.

The HAVIP unbound to a CVM cannot be published to the CCN. Please retry after binding it to a CVM.

Quota Limits

Resource	Limit
Number of route tables per VPC	10
Number of route tables associated with each subnet	1

Number of routing policies per route table	50
--	----

Creating Custom Route Tables

Last updated : 2024-10-22 15:44:56

A route table consisting of multiple routing policies is used to control the outbound traffic of the subnet. There are default route table and custom route tables. The default route table (local route) allows private network interconnection in the VPC, which cannot be deleted, but can be configured with routing policies the same way as you configure a custom route table. This document describes how to create and configure a custom route table.

Directions

1. Log in to the [VPC console](#).
2. Click **Route table** in the left sidebar to go to the route table management page.
3. Click **Create Policy**.
4. In the pop-up window, enter the route table name, select the VPC to which the route table belongs, and configure a routing policy.

Create Route Table

Name

60 more characters allowed

Network

vpc-

Advanced

Options

Routing Rules

Routing policies control the traffic flow in the subnet. For details, please see [Configuring Routing Policies](#).

Destination	Next hop type	Next hop	Notes	Operation
Local	LOCAL	Local	Delivered by default, indicates that C...	-
<div>such as 10.0.0.0/16</div>	<div>Public IP of CVM</div>	Public IP of CVM		

+Add a line

Create

Close

Note:

You can configure routing policies when creating a route table. Alternatively, after a route table is created, you can click the route table ID to go to the details page of the route table and click **+ Add routing policies** to configure routing policies.

Configuring a routing policy :

Parameter	Description
Destination	<p>Specify the destination IP range to which you want to forward traffic. Configure it as follows: Enter an IP range. If you want to enter a single IP, set the mask to 32 (for example, `172.16.1.1/32`).</p> <p>The destination cannot be an IP range of the VPC where the route table resides, because the local route already allows private network interconnection in this VPC.</p> <p>Note:</p> <p>If you have deployed a TKE service in the VPC, when you configure the routing policy of the route table for the VPC subnet, the destination cannot be within the CIDR block range of the VPC, nor can it contain the container IP range. For example, if a VPC CIDR block is `172.168.0.0/16` and the container network CIDR block is `192.168.0.0/16`, when you configure the routing policy for the VPC subnet, the destination IP range cannot be in the range of `172.168.0.0/16`, and cannot contain `192.168.0.0/16`.</p>
Next hop type	<p>Indicates the egress of data packets for the VPC. Supported types:</p> <p>NAT Gateway: the traffic directed to a destination IP range is forwarded to a NAT Gateway.</p> <p>Peering connections: The traffic directed to a destination IP range is forwarded to the VPC peer of a peering connection.</p> <p>Direct Connect Gateway: the traffic directed to a destination IP range is forwarded to a direct connect gateway.</p> <p>High Availability Virtual IP: the traffic directed to a destination IP range is forwarded to an HA VIP.</p> <p>VPN Gateway: the traffic directed to a destination IP range is forwarded to a VPN gateway.</p> <p>Public IP of CVM: the traffic directed to a destination IP range is forwarded to the public IP (including EIPs) of a CVM instance in the VPC.</p> <p>CVM: the traffic directed to a destination IP range is forwarded to a CVM instance in the VPC.</p> <p>CDC local gateway: Tencent Cloud CDC communicates with the customer IDC by using a CDC local gateway.</p>
Next hop	Specify the next hop instance to which the traffic is redirected, such as a gateway or CVM IP.
Notes	Enter the route description for resource management. This parameter is optional.
New Line	You can click + New line to configure multiple routing policies, or click the deletion icon in the Operation column to delete the unnecessary routing policies. A custom route table should contain at least one routing policy.

5. After completing the configurations, click **Create**. Then the route table will be displayed in the list.

Route Table

All VPCs

Help of Route T

+ New

Please enter the Route

ID/Name	Type	Network	Associated sub...	Creation Time	Operation
rtb- <div></div>	Custom Table	vpc- <div></div>	2	2021-06-01 15:00:32	Delete <div>More</div>

Related Operations

Routing policies whose **Next hop type** is **High availability virtual IP** or **CVM** in the default or custom route tables can be manually published to or withdrawn from CCN.

1. Click the route table ID to enter the details page.

Details of rtb-

Help of Rout

Basic Information

Associated Subnets

Basic Information

Route table name

Network

vpc-

Route table ID

rtb-

Tag

None

Region

South China (Guangzhou)

Creation Time

2021-06-01 15:00:32

Type

Custom Table

+ New routing policies

Export

Destination Address

Destination	Next hop type	Next hop	Notes	Enable routing	Route Status in CCN	Operation
0/16	LOCAL	Local	Delivered by default, indicates that CVMs in the VPC are interconnected.	<div></div>	Published	<div>Withdraw from CCN</div>
.1/32	CCN	ccn-		<div></div>	-	<div>Publish to CCN</div>
.2/32	CCN	ccn-		<div></div>	-	<div>Publish to CCN</div>

2. You can perform the following operations as needed:

Click **Publish to CCN** to publish an enabled routing policy to CCN.

Click **Withdraw from CCN** to withdraw a custom routing policy that has been published to CCN.

Click **Edit** to modify a routing policy.

Click **Delete** to delete a disabled routing policy.

Associating or Disassociating Subnet

Last updated : 2024-10-22 15:45:49

After the route table is created, it needs to be associated with the subnet in order to control the outbound traffic of the subnet. This document describes how to associate the route table with or disassociate it from the subnet.

Associating with Subnet

1. Log in to the [VPC console](#).
2. Select **Route Tables** in the left sidebar to go to the management page.
3. There are two methods to associated with the subnet:

In the list, select the route table that needs to associate with the subnet, and click **More > Associated Subnets** in the **Operation** column.

Route Table

Guangzhou

All VPCs

Help of Route 1

+ New

Please enter the Route

ID/Name	Type	Network	Associated sub...	Creation Time	Operation
rtb-2zjp3dnw	Default route table	vpc-l4m0tc5p	3	2021-05-19 14:16:44	<div>Delete</div> <div>More</div>
					<div>Associated Subnets</div>

Click the route table ID to go to the details page, select **Associated Subnets** tab, and click **+Associate Subnet**.

Details of rtb-

Basic Information

Associated Subnets

+Associate Subnet

Subnet ID/name	Availability Zone	CIDR Block	Operation
subnet-j1pn7hw0	Guangzhou Zone 3	10. <div></div> .0/24	Disassociate

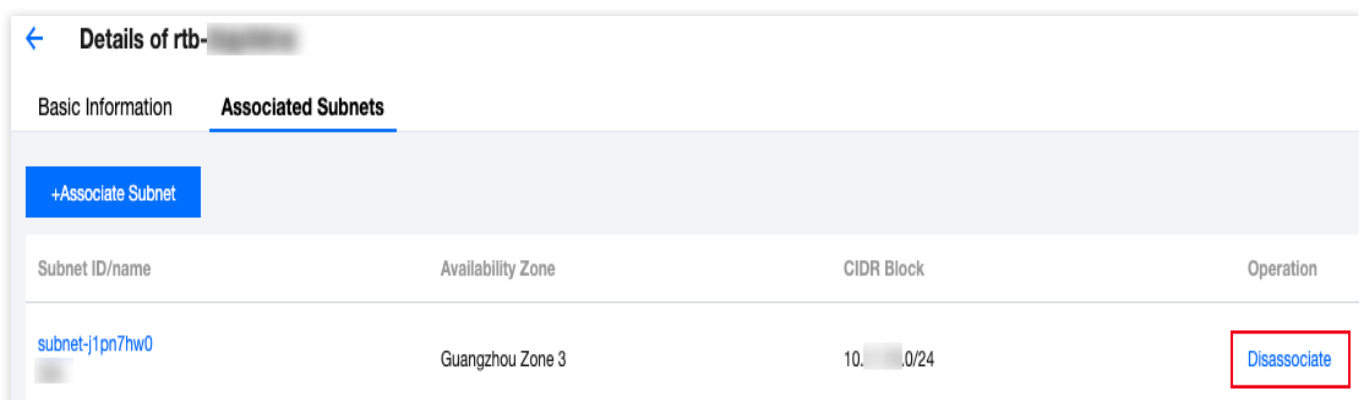
4. In the pop-up window, select the subnet to associate (a route table can be associated with multiple subnets at the same time, and you can quickly filter by subnet ID/name). Please evaluate the business impact of the association on the subnet. Confirm the impact, and click **OK**.

Note:

After the route table is associated with the subnet, the original route table associated with the subnet will be replaced with the new one, and the subnet outbound traffic will be executed according to the policies in the new route table. Please carefully evaluate the business impact.

Disassociating from Subnet

1. Log in to the [VPC console](#).
2. Select **Route Tables** in the left sidebar to go to the management page.
3. Click the route table ID to go to the details page, switch to the **Associated Subnets** tab, and click **Disassociate**.



4. In the pop-up window, select a new route table for the subnet to be disassociated, and click **OK** to complete the disassociation of the current route table from the subnet. The subnet outbound traffic policy will be executed based on the new route table selected for it.

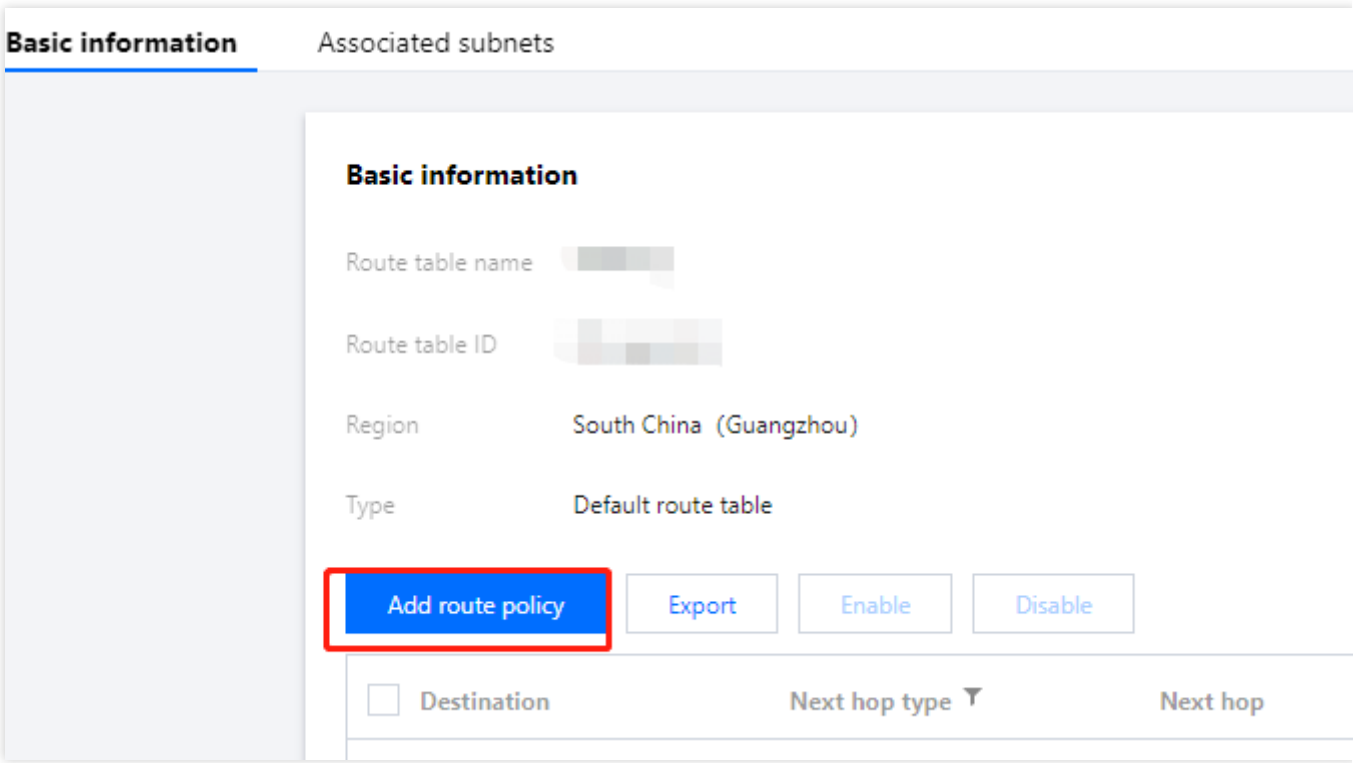
Managing Routing Policies

Last updated : 2024-10-22 15:46:09

The routing policies in a route table can be managed in real time. For example, you can add, delete, query, and export routing policies, publish routing policies to CCN, withdraw routing policies from CCN, and enable or disable routing policies. This document describes operations related to routing policies.

Adding a Routing Policy

1. Log in to the [VPC console](#), and access the **Route Table** page.
2. Click the **ID/Name** of the route table to modify to go to its details page.
3. Click **+ Add routing policies**.



4. In the pop-up window, configure the routing policy.

Note:

If you have deployed a [TKE service](#) in the VPC, the destination you configure in the routing policy of the VPC subnet cannot fall within the VPC CIDR block or contain the TKE IP range. For example, if the VPC CIDR block is `172.168.0.0/16` and the TKE CIDR block is `192.168.0.0/16`, the destination IP range cannot fall within `172.168.0.0/16`, or contain `192.168.0.0/16` when you configure routing policy for a VPC subnet.

Parameter	Description
Destination	<p>Specify the destination IP range to which you want to forward outbound traffic of the subnet. Requirements for a destination are as follows:</p> <p>The destination must be an IP range. If you want to enter a single IP, set the mask to `32` (for example, `172.16.1.1/32`).</p> <p>The destination cannot be an IP range of the VPC where the route table resides, because the local route already allows private network interconnection in this VPC.</p>
Next hop type	<p>Indicates the egress of data packets for the VPC. Supported types:</p> <p>NAT gateway: The traffic directed to a destination IP range is forwarded to a NAT gateway.</p> <p>Peering Connections: the traffic directed to a destination IP range is forwarded to the VPC peer of a peering connection.</p> <p>Direct Connect Gateway: the traffic directed to a destination IP range is forwarded to a direct connect gateway.</p> <p>High Availability Virtual IP: the traffic directed to a destination IP range is forwarded to an HAVIP.</p> <p>VPN Gateway: the traffic directed to a destination IP range is forwarded to a VPN gateway.</p> <p>Public IP of CVM: the traffic directed to a destination IP range is forwarded to the public IP (including EIPs) of a CVM instance in the VPC.</p> <p>CVM: the traffic directed to a destination IP range is forwarded to a CVM instance in the VPC.</p> <p>CDC local gateway: Tencent Cloud CDC communicates with the customer IDC by using a CDC local gateway.</p>
Next hop	Specify the next hop instance to which the traffic is redirected, such as a gateway or CVM IP.
Notes	Enter the route description for resource management. This parameter is optional.
New Line	You can click + New line to configure multiple routing policies, or click the deletion icon in the Operation column to delete the unnecessary routing policies.

Add a route

Routing policies control the traffic flow in the subnet. For details, please see [Configuring Routing Policies](#).

Destination	Next hop type	Next hop	Remark	Operation
<input type="text" value="such as 10.0.0.0/16"/>	<input type="text" value="Public IP of CVM"/>	Public IP of CVM①	<input type="text"/>	

[+ New line](#)

Create

Close

5. Click **Create**.

Editing a Routing Policy

1. Log in to the [VPC console](#), and access the **Route Table** page.
2. In the list, click the **ID/Name** of the target route table to go to its details page.
3. Click **Edit** in the **Operation** column of the routing policy to modify it.

Destination	Next hop type	Next hop	Notes	Enable routing	Route Status in CCN	Operation
v/16	LOCAL	Local	Delivered by default, indicates that CVMs in the VPC are interconnected.		Published	Withdraw from CCN
v/32	Public IP of CVM	Public IP of CVM	32		-	Publish to C
v/24	CCN	ccn-jcjb7u3p testx			-	Publish to CCN

4. Click **OK** to confirm the modification or **Cancel** to cancel the modification.

Publishing a Routing Policy to CCN or Withdrawing a Routing Policy from CCN

Routes of a VPC associated with a CCN are published to the CCN by default. For the new custom routing policies that are not published, you need to manually publish them. You can also withdraw a routing policy from CCN.

Currently, only the routing policies whose **Next hop type** is **High availability virtual IP** or **CVM** in the default or custom route tables can be manually published to or withdrawn from CCN.

Prerequisites

The VPC where the HAVIP or CVM resides is associated with a CCN instance.

Directions

1. Log in to the [VPC console](#), and access the **Route Table** page.
2. Click the **ID/Name** of the route table to modify to go to its details page.
3. Perform the following operations as needed:

Click **Publish to CCN** to manually publish a custom routing policy to CCN.

Click **Withdraw from CCN** to withdraw a custom routing policy that has been published to CCN.

Note:

A disabled routing policy cannot be published to CCN.

A routing policy cannot be disabled once being published to CCN.

Querying and Exporting a Routing Policy

1. Log in to the [VPC console](#), and access the **Route Table** page.
2. Click the **ID/Name** of the target route table to go to its details page. On this page, you can view the routing policies in this route table.
3. In the top-right search box, query the routing policies by entering a destination address.

+ New routing policies		Export		<input type="text" value="10.0.0.0/16"/>		
Destination	Next hop type	Next hop	Notes	Enable routing	Route Status in CCN	Operation
<input type="text" value="10.0.0.0/16"/>	LOCAL	Local	Delivered by default, indicates that CVMs in the VPC are interconnected.	<input checked="" type="checkbox"/>	Published	Withdraw from CCN

4. Click **Export** to save the search result in the .csv format.

Enabling/Disabling a Routing Policy

A custom routing policy can be enabled or disabled.

Directions

1. Log in to the [VPC console](#), and access the **Route Table** page.
2. Click the **ID/Name** of the target route table to enter its details page. Check the routing policy status:

 : enabled

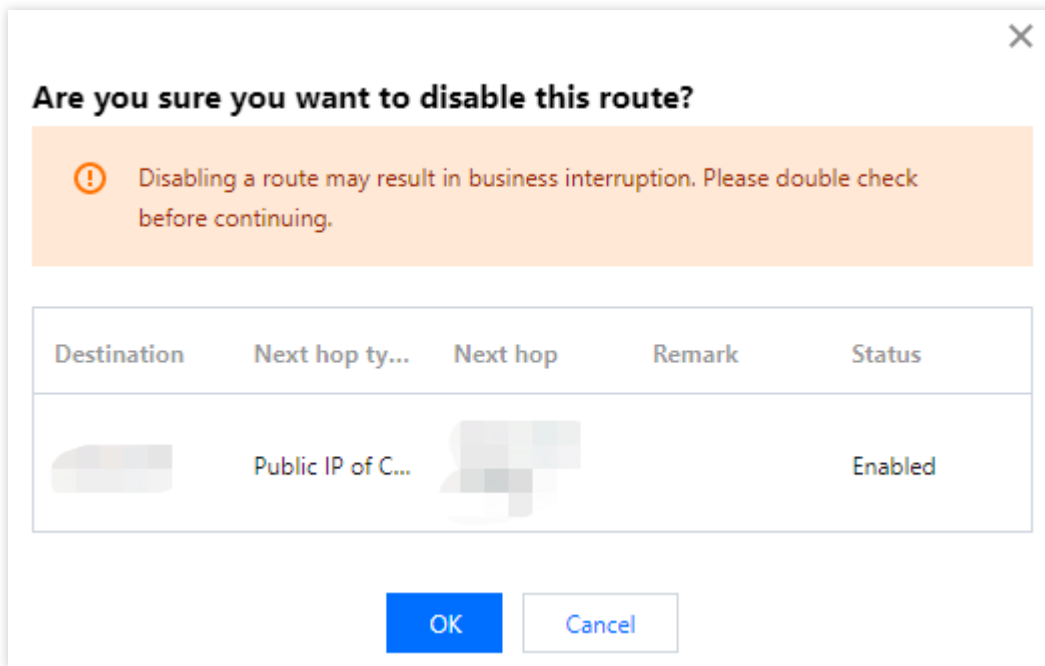
 : disabled

3. Disable a routing policy: click the

 icon next to a routing policy to disable it.

Note:

Disabling a route may result in business interruption. Please double check before continuing.



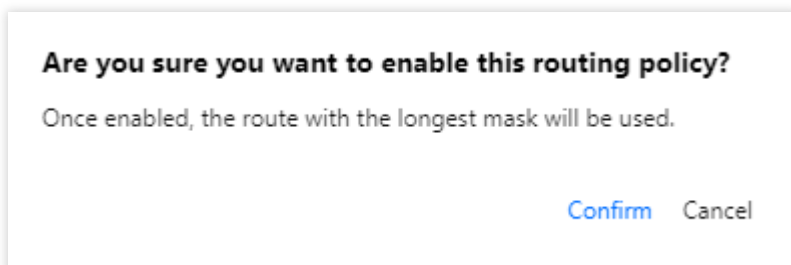
4. Enable a routing policy: click the



icon next to a routing policy to enable it.

Note:

Once enabled, the route with the longest mask will be used. This may affect your current business. Please double check before continuing.



5. Enable or disable multiple routing policies: select the target routing policies and click **Enable** or **Disable** above the list.

Add route policy

Export

Enable

Disable

Destination address

<input checked="" type="checkbox"/> Destination	Next hop type ▾	Next hop	Remark	Enable routing	Route status in CCN	Operation
<input type="checkbox"/>				<input type="checkbox"/>	-	Publish to CCN
<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>	-	Edit Delete Publish to C
<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>	-	Edit Delete Publish to C

Total items: 3

20 ▾ / page

⏪

◀

1

/ 1 page

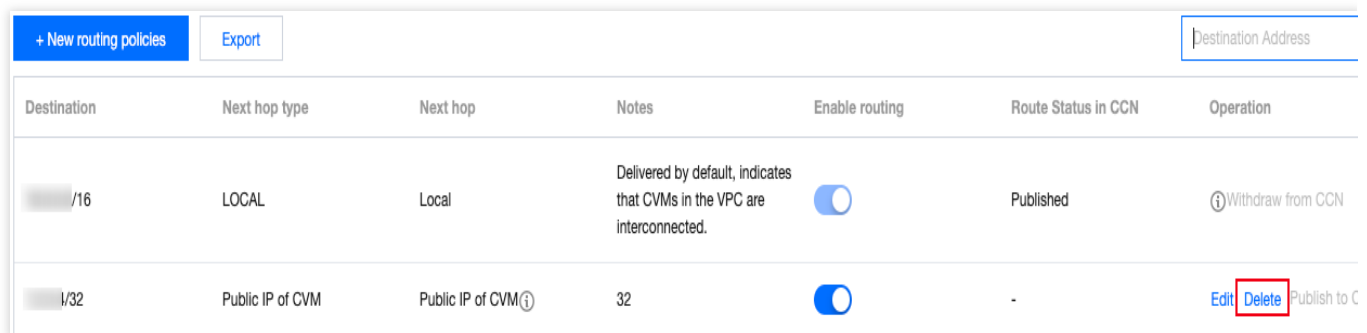
▶

⏩

Deleting a Routing Policy

You can delete the unused routing policies. Only the custom routing policies can be deleted.

1. Log in to the [VPC console](#), and access the **Route Table** page.
2. Click the **ID/Name** of the route table to modify to go to its details page.
3. Select the routing policy to be deleted, and click **Delete** in the **Operation** column.



+ New routing policies		Export	Destination Address			
Destination	Next hop type	Next hop	Notes	Enable routing	Route Status in CCN	Operation
/16	LOCAL	Local	Delivered by default, indicates that CVMs in the VPC are interconnected.	<input checked="" type="checkbox"/>	Published	Withdraw from CCN
/32	Public IP of CVM	Public IP of CVM	32	<input checked="" type="checkbox"/>	-	Edit Delete Publish to C



4. Read the notes and click **OK**.

×

Are you sure you want to delete this route?

!

Deleting a route may cause service interruption. Please double check before continuing.

Destination	Next hop ty...	Next hop	Remark	Status
	Public IP of C...			Enabled

OK

Cancel

Deleting a Routing Table

Last updated : 2024-10-22 15:46:29

You can delete the route table that is not associated with any subnet. You can only delete custom route tables, not the default route table which is automatically generated by the system.

Directions

1. Log in to the [VPC console](#), and select **Route Tables**.
2. In the list, select the route table to delete. Click **Delete** in the **Operation** column.

The screenshot shows the 'Route Table' management interface in the Tencent Cloud VPC console. The interface includes a header with 'Route Table', a region selector (Guangzhou), and a VPC selector (All VPCs). Below the header is a '+ New' button and a search bar. The main content is a table listing route tables. The table has the following columns: ID/Name, Type, Network, Associated sub..., Creation Time, and Operation. Three route tables are listed: 'rtb-kxr7p1ie' (Custom Table, 0 subnets), 'rtb-juuq0816' (Custom Table, 0 subnets), and 'rtb-mhzam6j0' (Default route table, 2 subnets). The 'Delete' button in the Operation column for the first table is highlighted with a red box. A confirmation dialog is open over the dialog, asking 'Are you sure you want to delete this route table?' with 'OK' and 'Cancel' buttons. The 'OK' button is also highlighted with a red box.

ID/Name	Type	Network	Associated sub...	Creation Time	Operation
rtb-kxr7p1ie	Custom Table	vpc-kkdh5eax	0	2021-02-23 20:16:31	Delete More
rtb-juuq0816	Custom Table	vpc-hanyttgj	0		Delete More
rtb-mhzam6j0	Default route table	vpc-hanyttgj	2		OK Cancel More

IPs and ENIs

Elastic IP

Last updated : 2024-10-22 15:46:48

[Elastic IP \(EIP\)](#): an EIP is a static IP address designed for dynamic cloud computing. It is also a public IP address that remains unchanged in a region. With EIPs, you can quickly remap an address to another instance or a NAT gateway instance under your account to shield instance failures.

You can keep the EIP under your account until it is released. While the public IP can only be released with the CVM, the EIP can be decoupled from the CVM lifecycle and operate independently as a cloud resource. For example, if you need to retain a public IP that is strongly related to your business, you can convert it into an EIP and keep it under your account.

For the step-by-step operations of EIPs, see the “Directions” section in [Elastic IP](#).

HAVIPs

Overview

Last updated : 2024-12-24 11:43:57

A high availability virtual IP (HAVIP) is a private IP address assigned from the CIDR block of a VPC subnet. It is usually used together with high-availability software, such as Keepalived and Windows Server Failover Cluster, to build a highly available primary/secondary cluster.

Note:

HAVIP is currently in beta, and switching between primary/secondary servers may take 10 seconds. To try it out, please apply to be a beta user.

To guarantee the CVM high availability in a primary/secondary cluster, we recommend assigning CVMs to different hosts using [placement groups](#). For more information about the placement group, see [Placement Group](#).

The high availability software should support sending ARP messages.

Features

You can apply for multiple HAVIP addresses in the console for each VPC.

High-Availability Virtual IP Address (HAVIP) is enabled with switch range control capability by default. After HAVIP is created, it is necessary to specify the scope of CVM or ENI for HAVIP switching.

You must bind the HAVIP in CVM's configuration file.

Architecture and Principle

Typically, a high availability primary/secondary cluster consists of two servers: an active primary server and a standby secondary server. The two servers share the same VIP (virtual IP). The VIP can only work on one primary server at the same time. When the primary server fails, the secondary server will take over the VIP to continue providing services.

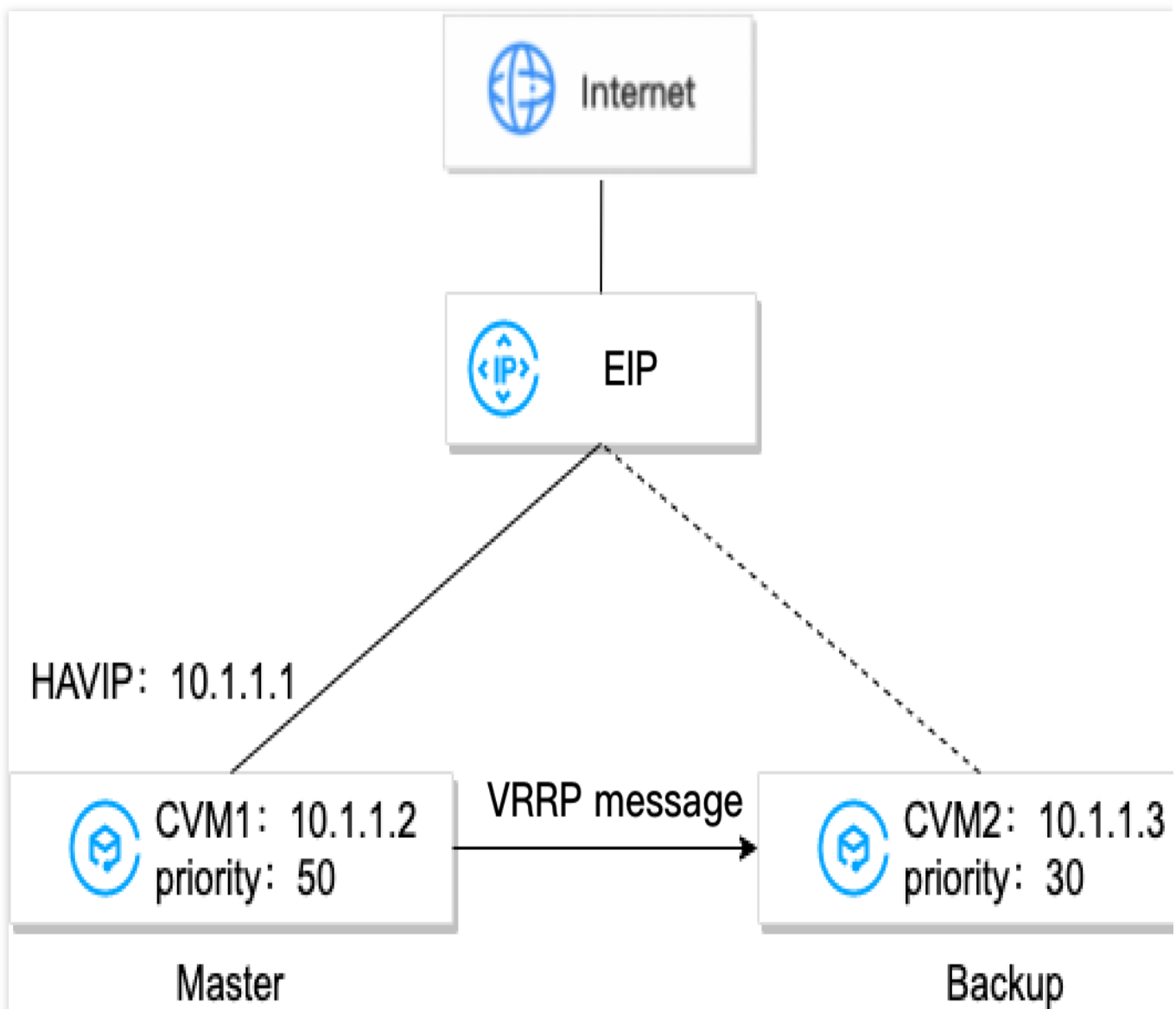
In traditional physical networks, the primary/secondary status can be negotiated with Keepalived's VRRP protocol. The primary device periodically sends free-of-charge ARP messages to purge the MAC table or terminal ARP table of the uplink exchange, so as to trigger the VIP migration to the primary device.

In a VPC, a high availability primary/secondary cluster can also be implemented by deploying Keepalived on CVMs. However, a CVM instance usually cannot obtain a private IP through ARP announcement due to security reasons such as ARP spoofing. The VIP must be a HAVIP applied from Tencent Cloud.

Note:

Keepalived is a VRRP-based high availability software. To use Keepalived, first complete its configuration in the `Keepalived.conf` file.

The following figure shows the HAVIP architecture.



According to the example figure, CVM1 and CVM2 can be built into a high availability primary/secondary cluster with the following steps:

1. Install Keepalived on both CVM1 and CVM2, configure HAVIP as VRRP VIP, and set the priorities of the primary and secondary servers. Larger values represent higher priorities.
2. Keepalived uses the VRRP protocol to compare the initial priorities of CVM1 and CVM2 and determines CVM1 as the primary server due to its higher priority.
3. The primary server sends out ARP messages, announces the VIP (a HAVIP), and updates VIP to mac mappings. In this case, the CVM1 is the primary server and provides services by using the private IP (HAVIP) for communication. You can see the HAVIP is bound to the primary server CVM1 on the HAVIP console.
4. (Optional) Bind an EIP to the HAVIP in the console to implement communication over the public network.

5. The primary server periodically sends VRRP messages to the secondary server. If the primary server fails to send VRRP messages within a certain period, the secondary server will be set as primary and sends out ARP update messages that carry its MAC address. In this case, CVM2 becomes the primary server to provide communication services and handle external access requests. You will see that the CVM bound to the HAVIP changes to CVM2 on the HAVIP console.

Common Use Cases

Cloud load balancer HA

To deploy Cloud Load Balancers (CLB), you will generally take HA between CLB instances and configure real servers as a cluster. Therefore, you must deploy and use HAVIP as a virtual IP between two CLB servers.

Relational database primary/secondary

If Keepalived or Windows Server Failover Cluster are used between two databases to build a highly available primary/secondary cluster, use HAVIP as a virtual IP. For more information, see [Building High Availability Primary/Secondary Cluster by Using HAVIP + Keepalived](#) and [Creating a High-availability Database by Using HAVIP + Windows Server Failover Cluster](#) under Best Practices.

FAQs

Why should I use HAVIP along with Keepalived in a VPC?

Some public cloud vendors do not support binding a private IP to CVM through ARP announcement due to security reasons such as ARP spoofing. If you directly use a private IP as virtual IP in the “Keepalived.conf” file, Keepalived will not be able to update the IP to MAC mapping during the primary/secondary server virtual IP switch. In this case, you have to call an API to switch the IP.

Using Keepalived configuration as an example, the IP configurations are as follows:

```
vrrp_instance VI_1 {
    state BACKUP                #Secondary device
    interface eth0               #ENI name
    virtual_router_id 51
    nopreempt                   #Non-preempt mode
    #preempt_delay 10
    priority 80
    advert_int 1
    authentication {
        auth_type PASS
        auth_pass 1111
    }
    unicast_src_ip 172.17.16.7   #Private IP of the local device
}
```

```
unicast_peer {
    172.17.16.13          #IP address of the peer device, for example: 10.0.0.
}

virtual_ipaddress {

    172.17.16.3  #Enter the HAVIP address you have applied for in the console.

}

garp_master_delay 1
garp_master_refresh 5

track_interface {
    eth0
}

track_script {
    checkhaproxy
}
}
```

If there is no HAVIP, the following section of the configuration file will be invalid.

```
virtual_ipaddress {
    172.17.16.3 #Enter the HAVIP address you have applied for in the console.
}
```

Reference

For more information about the use limits of HAVIP, see [Limits](#).

For more information about the operation guide of HAVIP, see [Managing HAVIP](#).

Limits

Last updated : 2024-12-17 17:52:27

Use Limits

The occupation of an HAVIP can be declared by the backend CVM, but you cannot manually bind HAVIPs to a specified server in the console (the experience is consistent with that of a traditional physical machine.)

The backend RS but not the HAVIP determines whether to migrate based on the configuration file negotiation.

Only VPC instances are supported, and the basic network is not supported.

Heartbeat detection must be done by an application on the CVM, but not by the HAVIP, which serves only as a floating IP address declared by ARP (the experience is consistent with that of a traditional physical machine.)

The HAVIP unbound to a CVM cannot be published to the CCN. Please retry after binding it to a CVM. For more information, see [Remarks](#).

The switch range limitation capability is enabled for HAVIP by default. If you need to disable it, please submit a [ticket](#).

Quota Limits

Resource	Limit
Default HAVIP quota in each VPC	10
Default quota of CVMs to bind with each HAVIP	20
Default quota of ENIs to bind with each HAVIP	50

Managing HAVIP

Last updated : 2024-12-17 17:55:39

This document describes how to create a HAVIP on the VPC console and configure it in third-party software.

Directions





1. Log in to the [VPC console](#) and select **IP and ENI** > **HAVIP** on the left sidebar.
2. Select the target region on the HAVIP management page and click **Apply**.
3. In the pop-up dialog box, configure HAVIP parameters.

Name: Enter a name for the HAVIP.

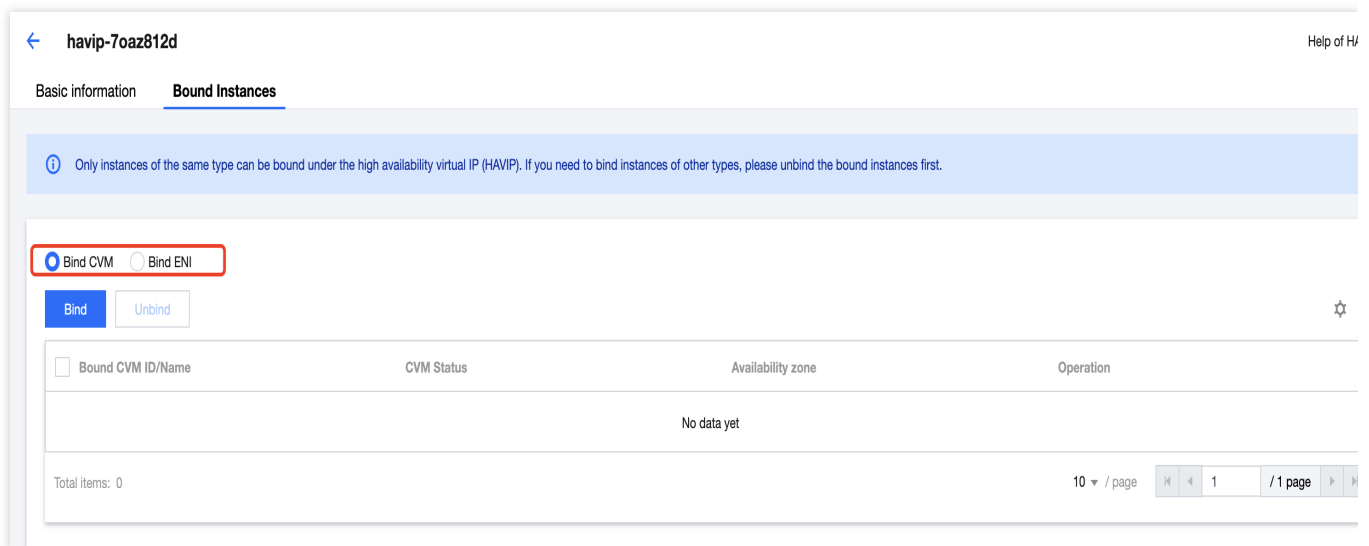
VPC: select a VPC where the HAVIP to be created resides.

Subnet: Select a subnet for the HAVIP.

- IP address:** The IP address of the HAVIP can be automatically assigned or manually specified. If you choose **Automatic Assignment**, a subnet IP address will be automatically assigned. If you choose **Enter manually**, make sure that the entered IP address is within the subnet IP range and is not a reserved IP address of the system. For example, if the subnet IP range is `10.0.0.0/24` , the entered private IP address should be within `10.0.0.2-10.0.0.254` .
4. Click **OK**. After the HAVIP is successfully created, it will be displayed in the list, with the main status information as follows.

ID/Name	Address	Switching Range Limit	Backend ENI	Effective Server	EIP	Network	Subnet	Application time	Update at	Operation
havip- 	10.	On 	-	-	-	vpc- 	subnet- 	Dec 11, 2024 16:47:47 (UTC+08:00)	-	Bind EIP Re Unbind EIP Refresh bindi

5. Click the **HAVIP ID**, select the bound instance on the details page, and fill in the instance range to which the HAVIP can switch.

**Note:**

To avoid HAVIP being preempted by an unexpected CVM, causing a business exception, the switch range limitation capability is enabled by default after the HAVIP is created.

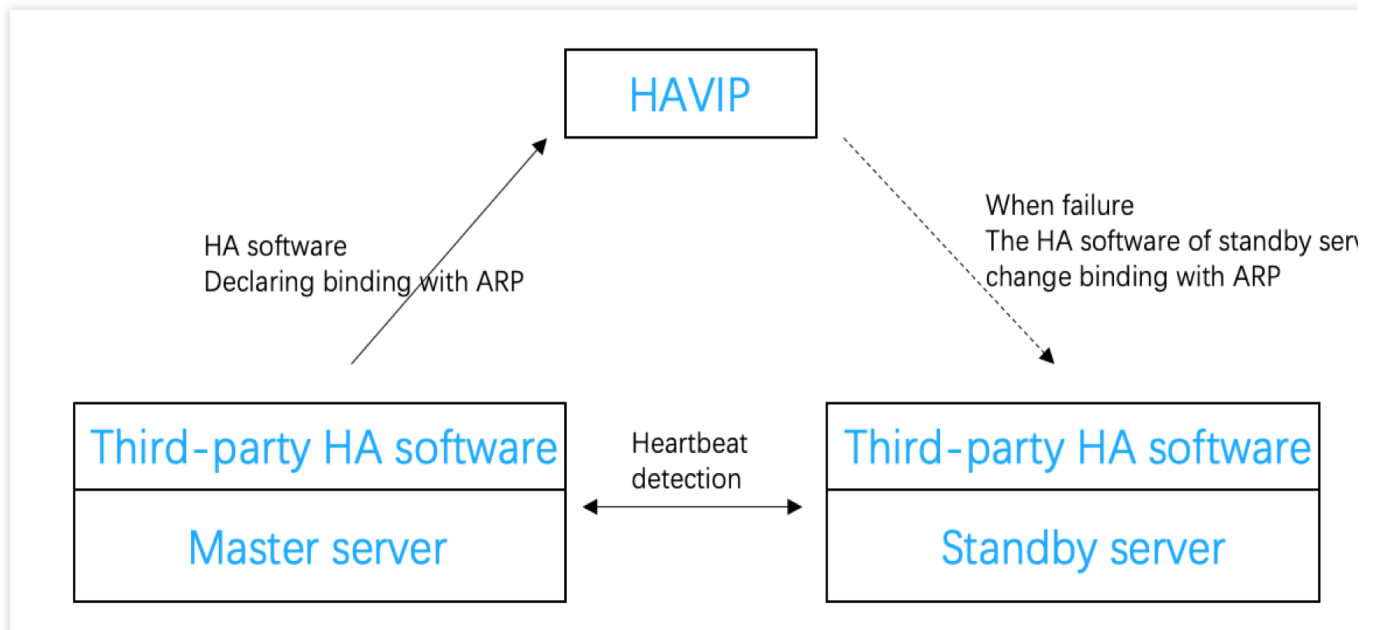
A HAVIP can only bind with the same type of instance. For example, CVM and ENI cannot be selected at the same time.

For binding ENIs, it currently only supports selecting ENIs already bound to CVM instances; the primary ENIs are not supported for binding.

When selecting the range of CVM, you can switch between all ENIs on the CVM, including the primary ENI.

Subsequent Operations

HAVIP is designed to use together with third-party HA software, which should be configured in third-party HA software. HAVIP is only an operation object and a private IP address that can be bound through announcement. Therefore, the binding and unbinding of HAVIP to CVMs are not done in the Tencent Cloud console. Instead, you only need to specify HAVIP as a floating virtual IP address (VIP) in the third-party HA software which in turn specifies an ENI to be bound to the HAVIP through ARP. The following shows you how to bind or unbind a HAVIP:



In a traditional physical device environment, all private IP addresses are bound to ENIs through ARP by default and can be specified as floating IP addresses in the HA software. In a public cloud environment, a private IP cannot use ARP, or be specified as a floating IP address in the HA software. Therefore, you need to follow the same steps as that of the third-party software to specify the HAVIP as a floating IP address instead.

Note:

Common HA software programs include: Linux HeartBeat, Keepalived, Pacemaker, and Windows MSCS.

When specifying a VIP in the configuration file of the HA software, you only need to enter the HAVIP that you created:

```

vrrp_instance VI_1 {
# Select proper parameters for the primary and secondary CVMs.
    state MASTER                #Set the initial status to `Backup`.
    interface eth0               #The ENI such as `eth0` used to bind a VIP
    virtual_router_id 51         #The `virtual_router_id` value for the cluster
        nopreempt               #Non-preempt mode
        preempt_delay 10        #Set the preempt delay to 10 minutes
    priority 100                 #Priority. The larger the value, the higher the prio
    advert_int 1                 #Check interval. The default value is 1 second
    authentication {             #Authentication
        auth_type PASS          #Authentication method
        auth_pass 1111          #Authentication password
    }

    unicast_src_ip 172.16.16.5    #Private IP address of the local device
    unicast_peer{
        172.16.16.6              #IP address of the peer device
    }
    virtual_ipaddress {
        172.16.16.12             #Set the "HAVIP" as a floating IP
    }
}
  
```

After the HAVIP is configured in the HA software of the CVM, the status of the HAVIP in the console will display the **backend ENI** and **effective server information**.

See the following cases for your configurations:

[Building High Availability Primary/Secondary Cluster by Using HAVIP + Keepalived](#) under Best Practices

[Creating a High-availability Database by Using HAVIP + Windows Server Failover Cluster](#) under Best Practices

Relevant Documentation

Similar to a private IP, a HAVIP can also be bound with or unbound from an EIP on the VPC console. If you need public network communication, see [Binding or Unbinding EIP](#).

Binding or Unbinding EIP

Last updated : 2024-12-17 17:52:27

Similar to a private IP, HAVIP binding can also be configured in the console. Binding a HAVIP refers to EIP operations. You can skip this section if no public network connection is needed.

Binding an EIP

1. Log in to the [VPC console](#) and select **IP and Interface** > **HAVIP** on the left sidebar.
2. Select the target region on the HAVIP management page.
3. Select the HAVIP to be bound with EIP, and click **Bind** under the **Operation** column.
4. In the pop-up dialog box, select an EIP to be bound.

Note:

An HAVIP can only be bound with one EIP. If no EIP is available, you must first create an EIP in the console.

If the HAVIP is not bounded with a CVM instance, the corresponding EIP will be in idle status and will incur an idle fee.

Please configure the HAVIP correctly and bind it to an instance by referring to the following cases:

[Building High Availability Primary/Secondary Cluster by Using HAVIP + Keepalived](#) under Best Practice

[Creating a High-availability Database by Using HAVIP + Windows Server Failover Cluster](#) under Best Practice

5. Click **OK**.

Unbinding an EIP

1. Log in to the [VPC console](#) and select **IP and Interface** > **HAVIP** on the left sidebar.
2. Select the target region on the HAVIP management page.
3. Select the HAVIP from which EIP will be unbound, and click **Unbind** under the **Operation** column.
4. In the pop-up, read the notes, and click **OK** to unbind the EIP.

Note:

Your public network business may be affected after unbinding the EIP. Please get ready in advance.

After being unbound, the EIP will be idle and incur an idle fee. You can directly release unused EIPs to avoid costs.

Querying HAVIPs

Last updated : 2024-12-17 17:52:27

You can view all HAVIP details in a specific region on the HAVIP console.

How It Works

- 1. Log in to the [VPC console](#).
- 2. Select **IP and ENI** > **HAVIP** on the left sidebar to enter the HAVIP management page.
- 3. Select a target region.

ID/Name	Address	Switching Range Limit	Backend ENI	Effective Server	EIP	Network	Subnet	Application time	Update at	Operation
hvip-...	10.	On	-	-	-	vpc-...	subnet-...	Dec 11, 2024 16:47:47 (UTC+08:00)	-	Bind EIP Re... Unbind EIP Refresh bindi

The field description is as follows:

ID/Name: An ID is generated automatically when an HAVIP is created. You can set a custom name for the HAVIP. Click on the ID to view the basic information of the HAVIP.

Address: HAVIP address.

Switch Range Limitation: Indicates whether the HAVIP switch range limitation capability is enabled. Once enabled, HAVIP can only switch within the specified instance range. New HAVIPs are enabled by default.

Backend ENI: ENI ID of the bound CVM. If it is not bound with a CVM, this field is -.

Effective Server: The CVM ID bound to HAVIP, namely the CVM ID associated with the backend ENI. If the HAVIP is not bound to a CVM, this will be displayed as -.

EIP: EIP bound with the HAVIP. If it is not bound with an EIP, this field is -.

Network: VPC of the HAVIP.

Subnet: Subnet of the HAVIP.

Application time: The time when this HAVIP is applied for.

Update Time: The last updated time of the ENI bound to the HAVIP.

Operation: Operations that HAVIP can perform, including: Bind EIP, Unbind EIP, Release, Refreshing binding relationship.

Bind EIP:binding elastic IP

Unbind EIP:unbinding elastic IP

Release:releasing HAVIP

Refreshing binding relationship:Reset the current binding relationship between HAVIP and the backend ENI.

Unbind EIP:

4. Enter ID, name or address in the search box on the right to quickly search for HAVIPs.
5. Click the icon next to the search box to refresh the page.

Releasing HAVIPs

Last updated : 2024-12-17 17:52:27

This document describes how to release unused HAVIPs.

Prerequisites

Only HAVIP **not bound with CVM** can be released.

Note:

For HAVIP **bound with CVM**, you need to unbind HAVIP in the configuration file of the third-party HA software on CVM before releasing it on the console.

Directions

1. Log in to the [VPC console](#).
2. Select **IP and Interface** > **HAVIP** on the left sidebar. In the HAVIP list, locate the HAVIP to be released.
3. Click **Release** under the **Operation** column.
4. Click **Confirm** in the pop-up dialog box.

ENIs

Last updated : 2024-10-22 15:49:05

[Elastic Network Interface](#) (ENI) is bound to a CVM in a VPC and can be migrated freely among CVMs. ENIs help you configure management networks and create highly reliable network solutions.

You can bind multiple ENIs in the same availability zone to a CVM based on the CVM specifications to ensure a highly available network. You can also bind multiple private IP addresses to an ENI to deploy multiple IP addresses for a single CVM.

For the common operations of ENI, please see:

[Creating an ENI](#)

[Binding and Configuring CVMs](#)

[Unbinding from a CVM](#)

[Deleting an ENI](#)

[Binding Secondary Private IP Addresses](#)

[Releasing Secondary Private IP Addresses](#)

[Binding EIPs](#)

[Unbinding EIPs](#)

[Modifying Primary Private IPs](#)

[Changing the Subnet of an ENI](#)

Bandwidth Package

Last updated : 2024-10-22 15:49:26

Tencent Cloud Bandwidth Package (BWP) is a multi-IP aggregated billing method. This mode greatly saves your public network fees when your public network instances have traffic peaks at different times.

BWP offers a [monthly pay-as-you-go](#) billing manner.

Note

BWP is not only available to beta users. To join the beta, please contact your sales rep.

For common BWP operations, see:

[Viewing the Billable Bandwidth](#)

[Changing Billing Mode](#)

[Managing IP Bandwidth Packages](#)

[Managing Device Bandwidth Packages](#)

Network Connection

NAT Gateway

Last updated : 2024-10-22 15:49:45

A [NAT gateway](#) is a service that supports IP address translation and provides SNAT and DNAT capabilities. It can provide secure, high-performance Internet access service for resources in the VPCs. For example, it can provide a secure egress, accessing the public network for multiple CVMs which don't already have an access to the public network (Internet).

For the common operations of NAT gateway, please see:

[Getting Started](#)

[Modifying NAT Gateway Configuration](#)

[Managing EIPs of NAT Gateway](#)

[Managing Port Forwarding Rules](#)

[Configuring a Route Pointing to NAT Gateway](#)

VPN Connection

Last updated : 2024-10-22 15:50:02

[VPN connection](#) is a private connectivity service based on IPSEC-based network tunneling which provides an encrypted and secure Site-to-Site connection between remote sites such as IDCs and resources in Tencent Cloud. The VPN connection makes it possible to securely access and exchange confidential data over shared network infrastructure, such as the public network (Internet).

For the common VPN operations, please see:

[VPN Gateway](#)

[Customer Gateway](#)

[VPN Tunnel](#)

[Connecting VPC to IDC \(Policy-Based Routing\)](#)

[Connecting VPC to IDC \(Route Table\)](#)

[Connecting IDC to CCN](#)

Direct Connect

Last updated : 2024-10-22 15:50:18

Direct Connect provides a fast and secure approach to connect Tencent Cloud networks with on-premises IDCs. It is based on TCP/IP Layer 2 dedicated channels which terminate on the Cloud based Direct Connect Gateway. From here you can access Tencent Cloud resources in multiple regions offering a flexible and reliable hybrid cloud environment.

For the common operations of Direct Connection, please see:

[Quick Start](#)

[Managing Connections](#)

[Managing Direct Connect Gateways](#)

[Dedicated Tunnels](#)

[Migrating IDC to the Cloud Through CCN](#)

Cloud Connect Network

Last updated : 2024-10-22 15:53:52

[Cloud Connect Network](#) (CCN) is a global private connectivity service running on top of the Tencent Cloud network backbone. CCN allows connectivity between VPCs in all regions, IDCs through VPN or Direct Connect links and even other Cloud or service providers. CCN's multi-level routing is capable of autonomous learning, so when the network topology changes, you do not need to perform tedious network based operations.

For the common CCN operations, please see:

[Network Instance Interconnection in One Account](#)

[Network Instance Interconnection Crossing Account](#)

[Instance Management](#)

[Route Management](#)

[Bandwidth Management](#)

Security Management

Security Groups

Overview

Last updated : 2024-10-22 15:54:14

A security group is a virtual firewall that features stateful data packet filtering. It is used to configure the network access control of CVM, Cloud Load Balancer, TencentDB, and other instances while controlling their outbound and inbound traffic. It is an important means of network security isolation.

You can configure security group rules to allow or reject inbound and outbound traffic of instances within the security group.

Features

A security group is a logical group. You can add CVM, ENI, TencentDB, and other instances in the same region with the same network security isolation requirements to the same security group.

If a security group has no rules, it will reject all traffic by default, and you need to add rules to it to allow traffic.

Security groups are stateful. Inbound traffic you have allowed can automatically become outbound and vice versa.

You can modify security group rules at any time, and the new rules will take effect immediately.

Use Limits

For use limits and quotas of security groups, see [Use Limits Overview](#).

Security Group Rules

Components

A security group rule consists of:

Source or Destination: The source IP for an inbound rule, or the destination IP for an outbound rule. It can be an IP address, an IP range, or a security group. For more information, see [Adding a Security Group Rule](#).

Protocol Type and Protocol Port: Protocol type, such as TCP and UDP.

Policy: Allow or reject.

Rule priorities

The rules in a security group are prioritized from top to bottom. The rule at the top of the list has the highest priority and will take effect first, while the rule at the bottom has the lowest priority and will take effect last.

If there is a rule conflict, the rule with the higher priority will prevail by default.

When traffic goes in or out of an instance bound to a security group, the security group rules will be matched sequentially from top to bottom. If a rule is matched successfully and takes effect, the subsequent rules will not be matched.

Multiple security groups

An instance can be bound to one or multiple security groups. When it is bound to multiple security groups, these security groups are executed from top to bottom. You can adjust their priorities at any time.

Security Group Templates

Tencent Cloud provides the following two security group templates:

Open all ports: All inbound and outbound traffic will be allowed to pass.

Open major ports: Port TCP 22 (for Linux SSH login), ports 80 and 443 (for web service), port 3389 (for Windows remote login), the ICMP protocol (for ping commands), and the private network (for the VPC IP range) will be open to the internet.

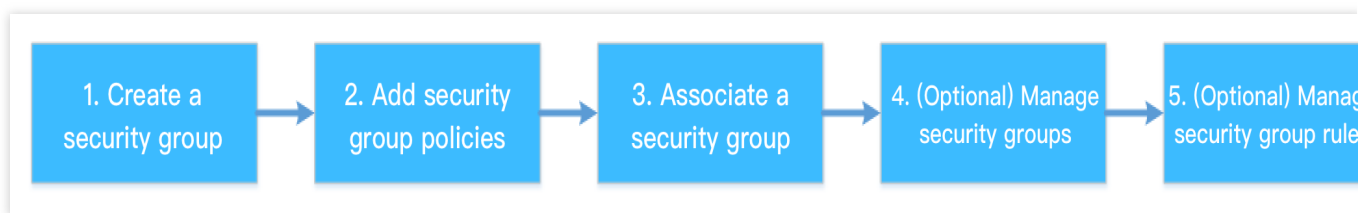
Note:

If these templates cannot meet your actual needs, you can create custom security groups. For more information, see [Creating a Security Group](#) and [Application Cases of Security Groups](#).

If you need to protect the application layer (HTTP/HTTPS), you can purchase [Tencent Cloud Web Application Firewall \(WAF\)](#), which provides web security at the application layer to defend against web vulnerabilities, malicious crawlers, and CC attacks, protecting your websites and web applications.

Directions

The following figure shows how to use a security group:



Security Group Best Practices

Creating security group

We recommend you specify a security group when purchasing a CVM instance via the API; otherwise, the default security group will be used. The default security group cannot be deleted. It adopts the default security rule (i.e., allowing all IPv4 addresses), which can be modified as needed after the security group is created.

If you need to change the instance protection policy, we recommend you modify the existing rules instead of creating a security group.

Managing rules

Export and back up the security group rules before you modify them, so you can import and restore them if an error occurs.

To create multiple security group rules, use a [parameter template](#).

Associating security group

You can add instances with the same protection requirements to the same security group, instead of configuring a separate security group for each instance.

We recommend you not bind one instance to too many security groups, which may cause rule conflicts and result in network disconnection.

Security Group and Cloud Firewall

Tencent Cloud Firewall (CFW) is a native Tencent Cloud SaaS firewall that integrates different capabilities, including vulnerability scanning, IPS intrusion block, internet-wide threat intelligence, and advanced threat source analysis, making it the traffic security and policy management center in the cloud environment. It also serves as the first security portal for cloud business.

In practice, a security group is generally associated with Tencent Cloud products including CVM to implement the access control at the security group level. CFW is deployed in a VPC or the internet to implement the access control between VPCs or between Tencent Cloud

You can use CFW to implement access control when a security group is insufficient to support the following use cases:

1. You need to understand the exposure and vulnerability of CVM assets on the internet and strengthen protection against network vulnerabilities through IPS intrusion prevention and virtual patching features.
2. You need to control the proactive access to the internet by domain and enhance the business security.
3. You need to implement access control by region, for example, blocking all IPs outside the Chinese mainland quickly.

Creating a Security Group

Last updated : 2024-10-22 15:54:30

Operation Scenario

A security group is a virtual firewall for CVM instances. Each CVM instance must belong to at least one security group. Tencent Cloud provides two templates: **Open all ports to the Internet** and **Open ports 22, 80, 443, and 3389 and ICMP protocol to the Internet**. With these templates, you can create a default security group when creating a CVM instance if you have not yet created a security group.

If you do not want your CVM instance to join the default security group, you can create another security group in the CVM console as follows:

Steps

1. Log in to [CVM Console](#).
2. In the left sidebar, click **Security Group** to enter the security group management page.
3. On the security group management page, choose **Region** and click **+Create**.
4. In the **Create a security group** window that appears, complete the configuration, as shown in the following figure:

Create a security group

Template

Open all ports

Name

Open all ports-2019120517402373859

Project

Default Project

Notes

All ports open for both Internet and private network (HIGH-RISK)

[Display template rule](#)

OK

Cancel

Template: based on the services to be deployed for the CVM instances in the security group, select an appropriate template to simplify security group rule configuration, as described in the following table:

Template	Description	Scenario
Open all ports to the Internet	By default, all ports will be opened to the Internet and private network, which however may incur security risks.	-
Open ports 22, 80, 443, and 3389 and the ICMP protocol to the Internet	By default, ports 22, 80, 443, and 3389 and the ICMP protocol will be opened to the Internet. In addition, all ports will be opened to the private network.	The web service needs to be deployed for instances in the security group.
Custom	After creating a security group, you can add security group rules as required. For details about the operation, see Adding Security Group Rules .	-

Name: customize the name of a security group.

Project: by default, the **Default project** is selected. You can also specify another project to facilitate future management.

Remarks: briefly describe the security group to facilitate future management.

5. Click **OK** to finish creating the security group.

If you select the **Custom** template when creating a security group, click **Set rules now** after the creation to [add security group rules](#).

Adding a Security Group Rule

Last updated : 2024-10-22 15:54:52

Operation Scenario

Security groups are used to determine whether to permit access requests from the Internet or private networks. For security considerations, access denial is adopted in the inbound direction in most cases. If you select the "Open all ports to the Internet" or "Open ports 22, 80, 443, and 3389 and the ICMP protocol to the Internet" template when creating a security group, the system will automatically add security group rules for some communication ports based on the selected template.

This document describes how to add security group rules to allow or forbid CVMs in a security group to access the Internet or VPC instances.

Notes

Security group rules are divided into IPv4 and IPv6 security group rules.

Open all ports is applicable to both IPv4 and IPv6 security group rules.

Prerequisites

You have created a security group.

You know what Internet or private network access requests need to be permitted or rejected for your CVM instance.

For more use cases of security group rule settings, see [Security Group Use Cases](#).

Steps

1. Log in to [CVM Console](#).
2. In the left sidebar, click [Security Group](#) to enter the security group management page.
3. On the security group management page, choose **Region**, and locate the row of the security group for which you want to set rules.
4. In the operation column, click **Modify Rules**.
5. On the security group rule settings page, click **Add Rule**.

ty group rule page, click **Inbound rules**, and select one of the following modes based on your actual needs to complete the operation.

Note

The following operation examples use mode 2 (adding rules).

Mode 1 (open all ports): is applicable to scenarios in which ICMP protocol rules do not need to be set and operations can be done through ports 22, 3389, 80, 443, 20, and 21, as well as the ICMP protocol.

Mode 2 (adding rules): is applicable to scenarios in which multiple communication protocols, such as ICMP, need to be set.

6. In the **Add Inbound Rules** window that appears, set rules.

The main parameters required for adding a rule are as follows:

Type: the default value is "Custom". You can also select another system rule template, such as "Windows login", "Linux login", "Ping", "HTTP (80)", or "HTTPS (443)".

Source/Destination: the source (inbound rules) or destination (outbound rules) of traffic. Choose one of the following options:

Specified Source/Destination	Description
An IPv4 address or IPv4 address range	Specify it in CIDR notation (for example, <code>203.0.113.0</code> , <code>203.0.113.0/24</code> , or <code>0.0.0.0/0</code> , where <code>0.0.0.0/0</code> indicates that all IPv4 addresses will be matched).
An IPv6 address or IPv6 address range	Specify it in CIDR notation (for example, <code>FF05::B5</code> , <code>FF05:B5::/60</code> , <code>::/0</code> , or <code>0::0/0</code> , where <code>::/0</code> or <code>0::0/0</code> indicates that all IPv6 addresses will be matched).
Import security group ID: you can import the following security group IDs: Security group ID Another security group	The current security group refers to the CVMs associated with the security group. Another security group refers to the ID of another security group under the same project in the same region.
Import the IP address object or IP address group object in the parameter template	-

Protocol port: enter the protocol type and port range, or import a protocol port or protocol port group in the [parameter template](#).

Policy: the default value is "Permit".

Permit: permit access requests over the port.

Reject: discard data packets directly without returning any response.

Remarks: briefly describe the rule to facilitate future management.

7. Click **Finish**. Inbound rules are added to the security group.

8. On the security group rule page, click **Outbound Rules**, and add outbound rules to the security group by referring to [Step 5](#) to [Step 7](#).

Associating CVM Instances with Security Groups

Last updated : 2024-10-22 15:55:06

Operation Scenario

As an important network security isolation method, a security group is used to configure network access control for one or more CVMs. You can associate CVM instances with one or more security groups based on your business needs. This document describes how to associate a CVM instance with a security group in the console.

Prerequisites

A CVM instance has been created.

Steps

1. Log in to [CVM Console](#).
2. In the left sidebar, click [Security Group](#) to enter the security group management page.
3. On the security group management page, choose **Region**, and locate the row of the security group for which you want to set rules.
4. In the operation column, click **Manage instance** to enter the **Associate with Instance** page.
5. On the **Associate with Instance** page, click **Add Association**.
6. In the "Add Instance Association" window that appears, select the instance to be bound with the security group and click **OK**.

Subsequent Operations

To view all the security groups that you have created in a region, query the security group list.

For details about the operation, see [Viewing a Security Group](#).

If you do not want a CVM instance to belong to one or multiple security groups, remove it from them.

For details about the operation, see [Removing from a Security Group](#).

If your business no longer needs one or multiple security groups, you can delete them. After you delete a security group, all security group rules in it will also be deleted.

For details about the operation, see [Deleting a Security Group](#).

Managing Security Groups

Viewing Security Groups

Last updated : 2024-10-22 16:10:04

Overview

This document describes how to check security groups under a region.

Directions

List all security groups

1. Log in to the [security group console](#), and go to the security group management page.
2. Select a region to see a list of security groups under that region.

Search for a security group

You can search for security groups by specifying the group ID/name/tag or using a keyword.

1. Log in to the [security group console](#), and go to the security group management page.
2. On the Security Group Management page, select **Regions**.
3. Click the search box, select a type from the drop-down list.

Security group ID: Input the group ID and click



.

Security group name: Input the group name and click



.

Tag: Input a tag and click



.

Keyword: Input a keyword and click



.

Other Operations

To learn about how to search for security groups by using syntax, click



Removing Instances

Last updated : 2024-10-22 16:10:21

Operation Scenario

You can remove CVM instances from a security group based on your business needs.

Prerequisites

The CVM instance to be removed has joined two or more security groups.

Steps

1. Log in to [Security Group Console](#), enter the security group management page.
2. On the security group management page, choose **Region**, and locate the row of the security group from which you want to remove instances.
3. In the operation column, click **Manage instances** to enter the **Associate with Instance** page.
4. On the **Associate with Instance** page, select the instance to be removed and click **Remove from security group**.
5. In the window that appears, click **OK**.

Cloning a Security Group

Last updated : 2024-10-22 16:10:34

Operation Scenario

You may need to clone a security group in the following scenarios:

You have created a security group named sg-A in region A and want to apply sg-A rules to instances in region B. In this case, you can clone sg-A to region B instead of creating another security group in region B.

Your business needs to execute a new security group rule. In this case, you can clone the original security group for backup.

Notes

By default, only the inbound and outbound rules of a security group are cloned, but not the instances associated with the security group.

Security groups can be cloned between projects or regions.

Steps

1. Log in to [Security Group Console](#), enter the security group management page.
2. On the security group management page, choose **Region** and locate the row of the security group to be cloned.
3. In the operation column, click **More > Clone**.
4. In the "Clone Security Group" window that appears, select **Target Project** and **Target Region** for the cloning, enter a **New Name** for the security group, and click **OK**.

Deleting a Security Group

Last updated : 2024-10-22 16:10:50

Operation Scenario

If your business no longer needs one or multiple security groups, you can delete them. After you delete a security group, all security group rules in the group will also be deleted.

Prerequisites

The security group to be deleted is not associated with any instances. If it is associated with instances, remove them from the security group first. Otherwise, the security group cannot be deleted. For details about the operation, see [Removing from a Security Group](#).

Steps

1. Log in to [Security Group Console](#), enter the security group management page.
2. On the security group management page, choose **Region**, and locate the row of the security group to be deleted.
3. In the operation column, click **More > Delete**.
4. In the window that appears, click **OK**.

Adjusting the Priorities of Security Groups

Last updated : 2024-10-22 16:11:07

Overview

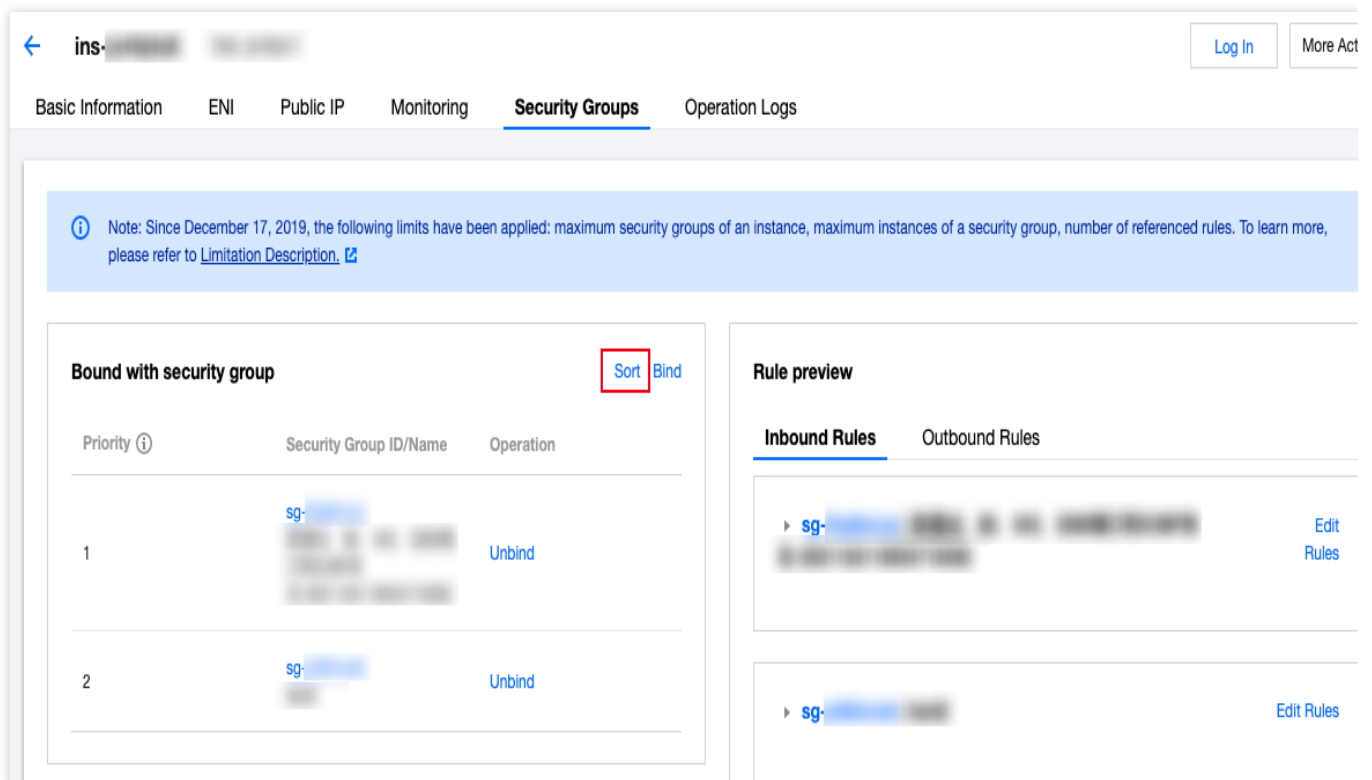
You can bind one or more security groups to a CVM. If you have bound multiple security groups, these security groups are executed based on their priorities. You can adjust the priorities as follows.

Prerequisites

The CVM instance is bound to two or more security groups.

Directions

1. Log in to the [CVM console](#).
2. On the instance management page, click the ID of the CVM instance to go to the details page.
3. Click the **Security Groups** tab to go to the security group management page.
4. In the **Bound Security Groups** module, click **Sort**.



ins-XXXXXX

Log In More Act

Basic Information ENI Public IP Monitoring **Security Groups** Operation Logs

Note: Since December 17, 2019, the following limits have been applied: maximum security groups of an instance, maximum instances of a security group, number of referenced rules. To learn more, please refer to [Limitation Description](#).

Bound with security group Sort Bind

Priority ⓘ	Security Group ID/Name	Operation
1	sg-XXXXXX	Unbind
2	sg-XXXXXX	Unbind

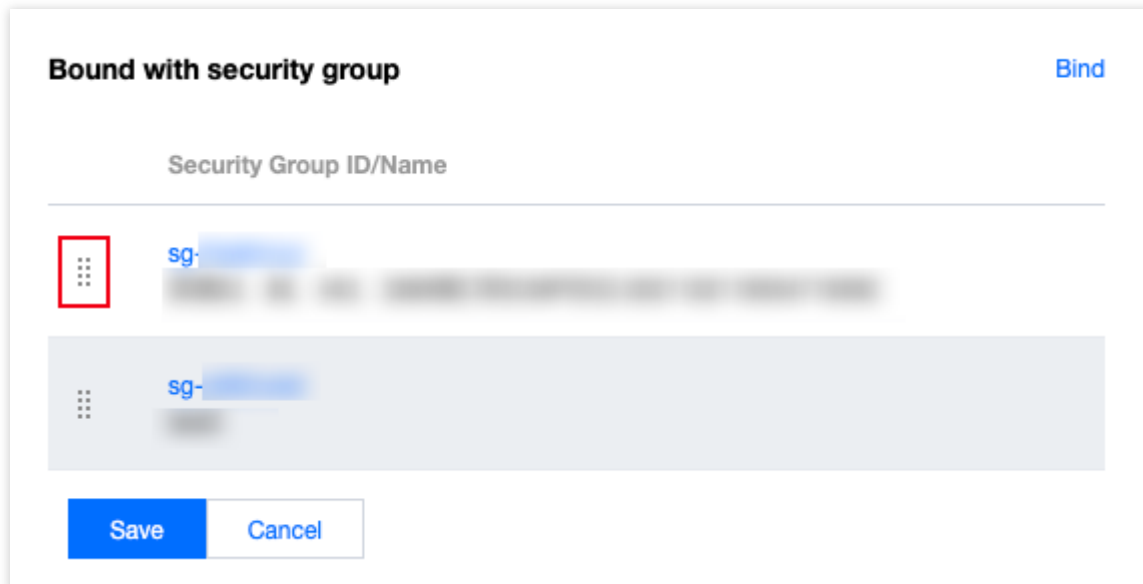
Rule preview

Inbound Rules Outbound Rules

sg-XXXXXX Edit Rules

sg-XXXXXX Edit Rules

5. Click the following icon and drag it up/down to adjust the priority of the security group. The higher the position, the higher the priority of the security group.



Bound with security group Bind

Security Group ID/Name

sg-XXXXXX

sg-XXXXXX

Save Cancel

6. After completing the adjustment, click **Save**.

Managing Security Group Rules

Viewing a Security Group Rule

Last updated : 2024-10-22 16:11:35

Operation Scenario

After adding a security group rule, you can view its details in the console.

Prerequisites

You have created a security group and added security group rules to the group.

For information on how to create a security group and add security group rules, see [Adding Security Group Rules](#).

Steps

1. Log in to [Security Group Console](#), enter the security group management page.
2. On the security group management page, choose **Region**, and locate the security group whose rules that you want to view.
3. Click the ID or name of the target security group to enter the security group rule page.
4. On the security group rule page, click the **Inbound Rules** or **Outbound Rules** tab to view the inbound or outbound rules of the security group.

Modifying a Security Group Rule

Last updated : 2024-10-22 16:11:52

Operation Scenario

Improperly set security group rules (for example, those that do not restrict access to specified ports) can incur severe security risks. In this case, you can modify these security group rules in a security group to ensure the network security of CVM instances. This document describes how to modify security group rules.

Prerequisites

You have created a security group and added security group rules to the group.

For information on how to create a security group and add security group rules, see [Creating a Security Group](#) and [Adding Security Group Rules](#).

Steps

1. Log in to [Security Group Console](#), enter the security group management page.
2. On the security group management page, choose **Region**, and locate the row of the security group whose rules are to be modified.
3. In the operation column, click **Modify Rules** to enter the security group rule page.
4. On the security group rule page, click the **Inbound Rules** or **Outbound Rules** tab based on the direction (inbound or outbound) of the security group rules to be modified.
5. Locate the security group rule that you want to modify and click **Edit** in the operation column to modify it.

Note:

You don't need to restart the CVM for the rule changes to take effect.

Deleting a Security Group Rule

Last updated : 2024-10-22 16:12:09

Operation Scenario

If you no longer need a security group rule, you can delete it.

Prerequisites

You have created a security group and added security group rules to the group.

For information on how to create a security group and add security group rules, see [Creating a Security Group](#) and [Adding Security Group Rules](#).

You have confirmed that your CVM instance does not need to permit or forbid Internet access or private network access.

Steps

1. Log in to [Security Group Console](#), enter the security group management page.
2. On the security group management page, choose **Region**, and locate the row of the security group whose rules are to be deleted.
3. In the operation column, click **Modify Rules** to enter the security group rule page.
4. On the security group rule page, click the **Inbound Rules** or **Outbound Rules** tab based on the direction (inbound or outbound) of the security group rules to be deleted.
5. Locate the security group rule that you want to delete and click **Delete**.
6. In the pop-up window, click **OK**.

Importing a Security Group Rule

Last updated : 2024-10-22 16:12:22

Overview

You can create and recover security group rules by importing backup rule file.

Directions

1. Log in to the [security group console](#), and enter the security group management page..
2. On the **Security Group** page, select a region and locate the target security group.
3. Click the ID/name of the security group.
4. Click **Inbound rule** or **Outbound rule**.
5. On the **Inbound Rule** or **Outbound Rule** tab, click **Import Rule**.
6. In the **Batch Import-Inbound/Outbound Rules** pop-up window, select the edited template file for the inbound/outbound rules and click **Import**.

Note:

Security group w/ rules: Click **Append** to add rules in the file before the existing rules.

Security group w/o rules: Download a template, edit the file, and import it.

For details about source and protocol port formats in the import rule template file, see the instructions on the console page.

Exporting a Security Group Rule

Last updated : 2024-10-22 16:12:36

Operation Scenario

You can export the security group rules of a security group for local backup.

Steps

1. Log in to [Security Group Console](#), enter the security group management page.
2. On the security group management page, choose **Region**, and locate the security group whose rules are to be exported.
3. Click the ID or name of the security group to enter the security group rule page.
4. On the security group rule page, click the **Inbound Rules or Outbound Rules** tab based on the direction (inbound or outbound) of the security group rules to be exported.
5. On the **Inbound Rules or Outbound Rules** tab page, click



in the upper-right corner to download and save the security group rule file to a local directory.

Sorting Security Group Rules

Last updated : 2024-10-22 16:12:56

Overview

Multiple security group rules can be added to a security group. They take effect in order from top to bottom and can be sorted as needed.

Prerequisites

You have created a security group with at least two rules as instructed in [Adding a Security Group Rule](#).

Directions

1. Log in to the [Security Group console](#) and enter the **Security Group** management page.
2. On the **Security Group** management page, select the **Region**.
3. Locate the target security group and click **Security Group ID** or **Modify Rule** in the **Operation** column to enter the **Security Group Rules** page.
4. On the **Security Group Rules** page, click **Sort**.
5. You can drag the following icon to sort the security group rules. The higher the position, the higher the priority. Then click **Save**.

Snapshot Rollback

Last updated : 2024-10-22 16:13:12

If a security group is configured with a snapshot policy, its rules will be backed up according to the configured policy. To roll back its rules, perform a snapshot rollback.

Prerequisites

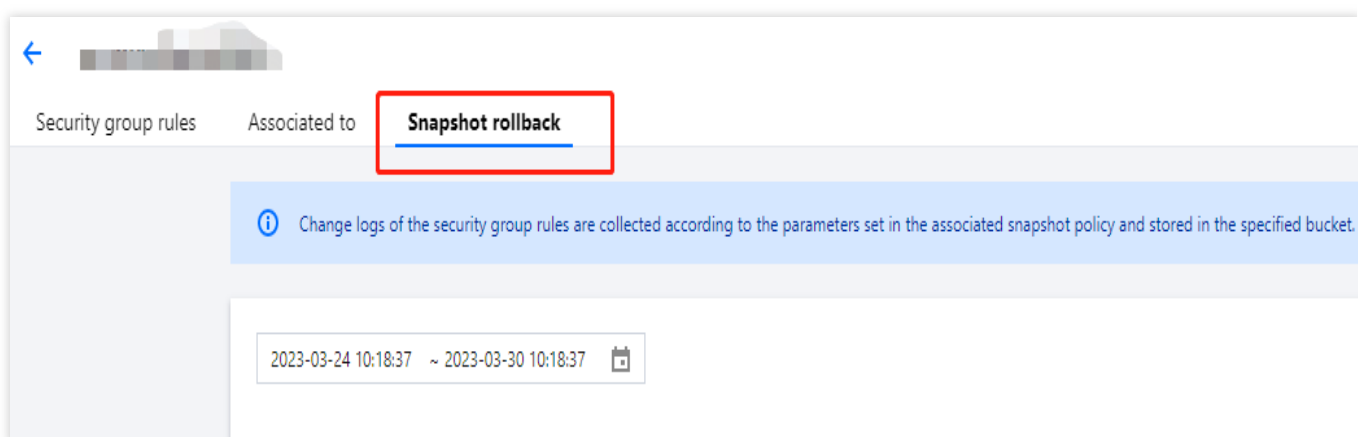
Configure a [snapshot policy](#) for the security group and create a snapshot backup.

Directions

1. Log in to the [Security Group console](#) and enter the **Security Group** management page.
2. On the **Security Group** management page, click the ID of the target security group to enter its details page.
3. Click the **Snapshot Rollback** tab, which displays all the snapshot records by time. By default, records from the past seven days are displayed. You can specify a query period.

Note:

If there are many backup records, we recommend you limit the time range to three months; otherwise, the system may become slow.



4. Click **Export** to export the inbound and outbound rules saved in this snapshot. Rules are separately in the **Inbound rules** and **Outbound rules** files.
5. Click **Restore** to enter the security group restoration page, which displays the security group rule preview and comparison.

Note:

+ indicates newly-added entries, while - means that the entry is deleted. The comparison result is based on the time period currently selected for comparison preview, during which if rules are changed, the comparison result may be

inaccurate.

When a security group is restored, if its source contains parameter template rules and nested security groups, the rules within the parameter template and the associated security group instance will remain in the current status.

Note that when you restore a security group with a snapshot, all current rules are overwritten.

6. Click **OK** to complete the rollback.

Application Cases of Security Groups

Last updated : 2024-10-22 16:13:30

Security groups are used to manage whether a Cloud Virtual Machine (CVM) is accessible. You can configure inbound and outbound rules for security groups to specify whether your server can be accessed by or can access other network resources.

Default inbound and outbound rules for security groups are as follows:

To ensure data security, the inbound rule for a security group is a rejection policy that denies remote access from external networks. To make your CVM accessible to external resources, you need to allow the inbound rule for the corresponding port.

The outbound rule for a security group specifies whether your CVM can access external network resources. If you select **Open All Ports** or **Open Ports 22, 80, 443, and 3389 and ICMP**, the outbound rule for the security group opens the ports to the Internet. If you select a custom security group rule, the outbound rule blocks all ports by default, and you need to set the outbound rule to allow the corresponding port to access external network resources.

Common Use Cases

This document describes several common use cases for security groups. If any of the following cases meet your requirements, you can set your security groups according to the configuration recommended for the corresponding use case.

Scenario 1: remotely connecting to a Linux CVM through SSH

Case: you have created a Linux CVM and want to remotely connect to the CVM through SSH.

Solution: when [adding an inbound rule](#), set **Type** to **Linux Login** and open TCP port 22 to the Internet to allow Linux login through SSH.

You can open all IP addresses or a specified IP address (or IP address range) to the Internet as required. This allows you to configure the source IP addresses that can remotely access the CVMs through SSH.

Direction	Type	Source	Protocol Port	Policy
Inbound	Linux login	All IP addresses: 0.0.0.0/0 Specified IP address: a specified IP address or IP address range	TCP: 22	Allow

Scenario 2: remotely connecting to a Windows CVM through RDP

Case: you have created a Windows CVM and want to remotely connect to the CVM through Remote Desktop Connection (RDP).

Solution: when [adding an inbound rule](#), set **Type** to **Windows Login** and open TCP port 3389 to the Internet to enable remote login to Windows.

You can open all IP addresses or a specified IP address (or IP address range) to the Internet as required. This enables you to configure the source IP addresses that can remotely access the CVMs through RDP.

Direction	Type	Source	Protocol Port	Policy
Inbound	Windows login	All IP addresses: 0.0.0.0/0 Specified IP address: a specified IP address or IP address range	TCP: 3389	Allow

Scenario 3: pinging a CVM from the Internet

Case: you have created a CVM and want to check whether the communication between the CVM and other CVMs is normal.

Solution: test the connection by using the ping program. Specifically, when [adding an inbound rule](#), set **Type** to **Ping** and open Internet Control Message Protocol (ICMP) ports to the Internet to enable other CVMs to gain access to this CVM through ICMP.

You can open all IP addresses or a specified IP address (or IP address range) to the Internet as required. This allows you to configure the source IP addresses that can access this CVM through ICMP.

Direction	Type	Source	Protocol Port	Policy
Inbound	Ping	All IP addresses: 0.0.0.0/0 Specified IP address: a specified IP address or IP address range	ICMP	Allow

Scenario 4: remotely logging in to a CVM through Telnet

Case: you want to remotely log in to a CVM through Telnet.

Solution: when [adding an inbound rule](#), configure the following security group rule:

Direction	Type	Source	Protocol Port	Policy
Inbound	Custom	All IP addresses: 0.0.0.0/0 Specified IP address: a specified IP address or IP address range	TCP: 23	Allow

Scenario 5: authorizing access to a web service through HTTP or HTTPS

Case: you have built a website and want to allow users to access your website through HTTP or HTTPS.

Solution: when [adding an inbound rule](#), configure the following security group rules as required:

Allow all IP addresses on the Internet to access this website

Direction	Type	Source	Protocol Port	Policy
Inbound	HTTP (80)	0.0.0.0/0	TCP: 80	Allow
Inbound	HTTPS (443)	0.0.0.0/0	TCP: 443	Allow

Allow some IP addresses on the Internet to access this website

Direction	Type	Source	Protocol Port	Policy
Inbound	HTTP (80)	The IP address or IP address range that is allowed to access your website	TCP: 80	Allow
Inbound	HTTPS (443)	The IP address or IP address range that is allowed to access your website	TCP: 443	Allow

Scenario 6: allowing an external IP address to access a specified port

Case: you have deployed a service and want the specified service port (such as port 1101) to be accessible externally.

Solution: when [adding an inbound rule](#), set **Type** to **Custom** and open TCP port 1101 to the Internet to allow external resources to access the specified service port.

You can open all IP addresses or a specified IP address (or IP address range) to the Internet as required. This allows the source IP address to access the specified service port.

Direction	Type	Source	Protocol Port	Policy
Inbound	Custom	All IP addresses: 0.0.0.0/0 Specified IP address: a specified IP address or IP address range	TCP: 1101	Allow

Scenario 7: denying access to a specified port from external IP addresses

Case: you have deployed a service and want to block external access to a specified service port (such as port 1102).

Solution: when [adding an inbound rule](#), set **Type** to **Custom**, configure TCP port 1102, and set **Policy** to **Reject** to deny external access to the specified service port.

Direction	Type	Source	Protocol Port	Policy
Inbound	Custom	All IP addresses: 0.0.0.0/0	TCP: 1102	Reject

		Specified IP address: a specified IP address or IP address range		
--	--	--	--	--

Scenario 8: allowing a CVM to access only a specified external IP address

Case: you want your CVM to access only a specified external IP address.

Solution: add two outbound security group rules by referring to the following configurations:

Allow the CVM instance to access a specified public IP address

Disallow the CVM instance to access any public IP addresses through any protocol

Note:

The rule that permits access should have a higher priority than the rule that denies access.

Direction	Type	Source	Protocol Port	Policy
Outbound	Custom	The specified public IP address that can be accessed by the CVM	The required protocol and port	Allow
Outbound	Custom	0.0.0.0/0	All	Reject

Scenario 9: denying a CVM from accessing a specified external IP address

Case: you do not want your CVM to access a specified external IP address.

Solution: add a security group rule by referring to the following configuration:

Direction	Type	Source	Protocol Port	Policy
Outbound	Custom	The specified public IP address that you do not want to be accessed by the CVM	All	Reject

Scenario 10: uploading a file to or downloading a file from a CVM through FTP

Case: you want to upload a file to or download a file from a CVM by using an FTP program.

Solution: add a security group rule by referring to the following configuration:

Direction	Type	Source	Protocol Port	Policy
Inbound	Custom	0.0.0.0/0	TCP: 20-21	Allow

Combination of Multiple Scenarios

In an actual scenario, you may want to configure multiple security group rules based on service requirements, for example, configuring inbound or outbound rules at the same time. One CVM may be bound to one or more security

groups. When a CVM is bound to multiple security groups, these security groups are matched and executed in descending order of priorities. You can adjust the priorities of these security groups whenever needed.

Common Server Ports

Last updated : 2024-10-22 16:13:48

The following describes the common server ports. For more information on service application ports for Windows, see the official Microsoft document ([Windows Service Overview and Network Port Requirements](#)).

Port Number	Service	Description
21	FTP	An open FTP server port for uploading and downloading.
22	SSH	Port 22 is the SSH port. It is used to remotely connect to Linux servers in CLI mode.
25	SMTP	SMTP server's open port for sending emails.
80	HTTP	This port is used for web services such as IIS, Apache, and Nginx to provide external access.
110	POP3	Port 110 is open for the POP3 (email protocol 3) service.
137, 138, 139	NetBIOS protocol	Ports 137 and 138 are UDP ports for transferring files through My Network Places. Port 139: connections over port 139 attempt to access the NetBIOS/SMB service. This protocol is used for file and printer sharing on Windows and SAMBA.
143	IMAP	Port 143 is mainly used for Internet Message Access Protocol (IMAP) v2, a protocol for receiving emails that is similar to POP3.
443	HTTPS	A web browsing port. HTTPS is another type of HTTP that provides encryption and transmission through secure ports.
1433	SQL Server	Port 1433 is the default port for SQL Server. SQL Server uses two ports: port 1433 for TCP and port 1434 for UDP. Port 1433 is used for SQL Server to provide external services, whereas port 1434 is used to respond to the requester regarding which TCP/IP port is being used by SQL Server.
3306	MySQL	Port 3306 is the default port for MySQL databases and is used to provide external services.
3389	Windows Server Remote Desktop Services	Port 3389 is the port for remote desktop service on Windows 2000/2003 Server, through which you can connect to a remote server by using the Remote Desktop connection tool.
8080	Proxy port	Similar to port 80, port 8080 is used for the WWW proxy service for web browsing.

The port number extension ":8080" is often appended to the URL when users visit a website or use a proxy server. In addition, after the Apache Tomcat web server is installed, the default service port is port 8080.

Network ACL

Rule Overview

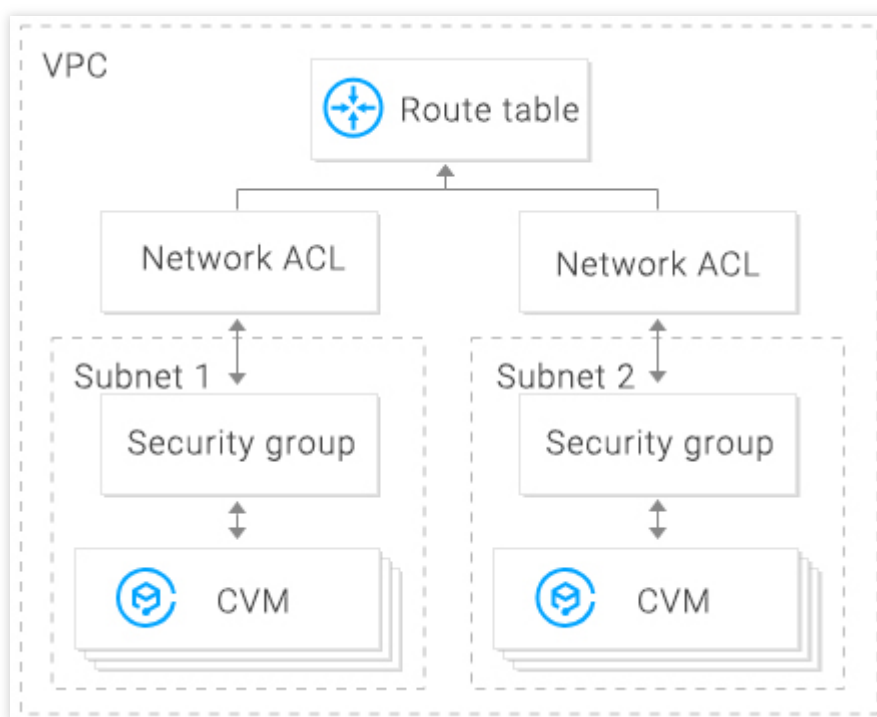
Last updated : 2024-10-22 16:14:08

The network Access Control List (ACL) is an optional layer of security that throttles traffic to and from subnets accurate to protocol and port.

Overview

You can associate a network ACL with multiple subnets to maintain the same traffic and precisely control their inflow and outflow by setting inbound and outbound rules.

For example, when you host a multi-layer web application in a Tencent Cloud VPC instance and create different subnets for web-layer, logic-layer, and data-layer services, you can use a network ACL to ensure that the web-layer and data-layer subnets cannot access each other, but only the logic-layer subnet can access the web-layer and data-layer subnets.



ACL Rules

When a network ACL rule is added or deleted, the change will be applied to the associated subnets automatically. You can configure inbound and outbound network ACL rules. Each rule consists of:

Source IP/destination IP: enter the source IP for an inbound rule or the destination IP for an outbound rule. Supported formats:

Single IP: such as "192.168.0.1" or "FF05::B5"

CIDR block: such as "192.168.1.0/24" or "FF05:B5::/60"

All IPv4 addresses: "0.0.0.0/0"

Protocol type: indicates protocol types that an ACL rule allows or denies, for example, TCP and UDP.

Port: indicates the source or destination port of traffic. Supported formats:

Single port: such as "22" or "80"

Port range: such as "1-65535" or "100-20000"

All ports: All

Policy: indicates whether to allow or deny the access request.

Default rules

Once created, every network ACL has two default rules that cannot be modified or deleted, with the lowest priority.

Default inbound rule

Protocol Type	Port	Source IP	Policy	Description
All	All	0.0.0.0/0	Deny	Denies all inbound traffic.

Default outbound rule

Protocol Type	Port	Destination IP	Policy	Description
All	All	0.0.0.0/0	Deny	Denies all outbound traffic.

Rule priorities

The rules of a network ACL are prioritized from top to bottom. The rule at the top of the list has the highest priority and will take effect first, while the rule at the bottom has the lowest priority and will take effect last.

If there is a rule conflict, the rule with the higher priority will prevail by default.

When traffic goes in or out of a subnet that is bound to a network ACL, the network ACL rules will be matched sequentially from top to bottom. If a rule is matched successfully and takes effect, the subsequent rules will not be matched.

Application example

To allow all source IP addresses to access all ports of CVMs in a subnet associated with a network ACL and deny HTTP source IP address of 192.168.200.11/24 to access port 80, add the following two network ACL rules for inbound traffic:

Protocol Type	Port	Source IP	Policy	Description
---------------	------	-----------	--------	-------------

HTTP	80	192.168.200.11/24	Deny	Denies this IP address of HTTP services to access port 80.
All	All	0.0.0.0/0	Allow	Allows all source IP addresses to access all ports.

Security Groups vs. Network ACLs

Item	Security Group	Network ACL
Traffic throttling	Traffic throttling at the instance level, such as CVM and database	Traffic throttling at the subnet level
Rule	Allow and deny rules	Allow and deny rules
Stateful or stateless	Stateful: returned traffic is automatically permitted without being subject to any rules.	Stateless: returned traffic must be explicitly permitted by rules.
Effective time	Rules are applied to an instance, such as a CVM or TencentDB, only if you specify a security group when creating the instance or associate a security group with the instance after it is created.	The ACL rules are automatically applied to all instances, such as CVM and TencentDB instances in the associated subnet.
Rule priority	If there is a rule conflict, the rule with the higher priority will prevail by default.	If there is a rule conflict, the rule with the higher priority will prevail by default.

Limits

Last updated : 2024-10-22 16:14:25

Use Limits

One network ACL can be bound with multiple subnets.
Network ACLs are stateless. Therefore, you need to set outbound rules and inbound rules respectively.
Network ACLs do not affect private network intercommunication among CVM instances in the associated subnets.

Quota Limits

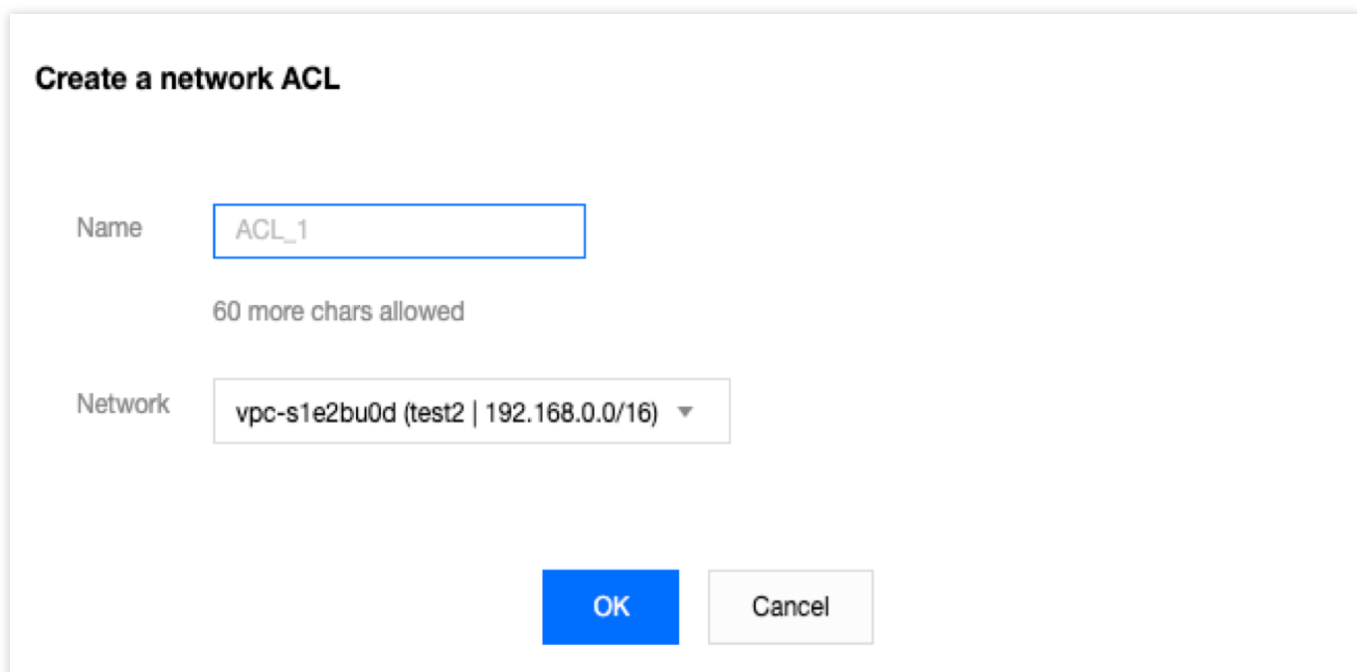
Resource	Limit
Number of network ACLs in each VPC	50
Number of rules per network ACL	Inbound: 20 Outbound: 20
Number of network ACLs associated with each subnet	1

Managing Network ACLs

Last updated : 2024-10-22 16:14:42

Creating Network ACLs

1. Log in to the [VPC console](#).
2. Click **Security** -> **Network ACL** in the directory on the left to go to the management page.
3. Select the region and VPC at the top of the list and click **+New**.
4. Enter its name in the pop-up window, select the VPC it belongs to, and click **OK**.



Create a network ACL

Name

60 more chars allowed

Network

OK **Cancel**

5. On the list page, click the ID of the corresponding ACL to go to its details page, where you can add ACL rules and associate ACL rules with subnets.

Adding Network ACL Rules

1. Log in to the [VPC console](#).
2. Click **Security** -> **Network ACL** in the directory on the left to go to the management page.
3. Look in the list for the network ACL to be modified, and click its ID to go to the details page.
4. To add an outbound/inbound rule, click **Outbound Rules** or **Inbound Rules** -> **Edit** -> **New Line**, select the protocol type, enter the port and source IP address, and select the policy.

Protocol type: indicates protocol types that an ACL rule allows or rejects, for example, TCP and UDP.

Port: indicates the source port of traffic, which can be a single port or a port segment, for example, port 80 or ports 90 to 100.

Source IP address: indicates the source IP address or IP range of traffic that supports the IP range or CIDR block, for example, `10.20.3.0` or `10.0.0.2/24`.

Policy: allows or rejects the access request.

The screenshot shows the 'Inbound rule' configuration page in the Tencent Cloud VPC console. The 'Inbound rule' tab is selected. The 'Rule list' table contains one rule with the following details:

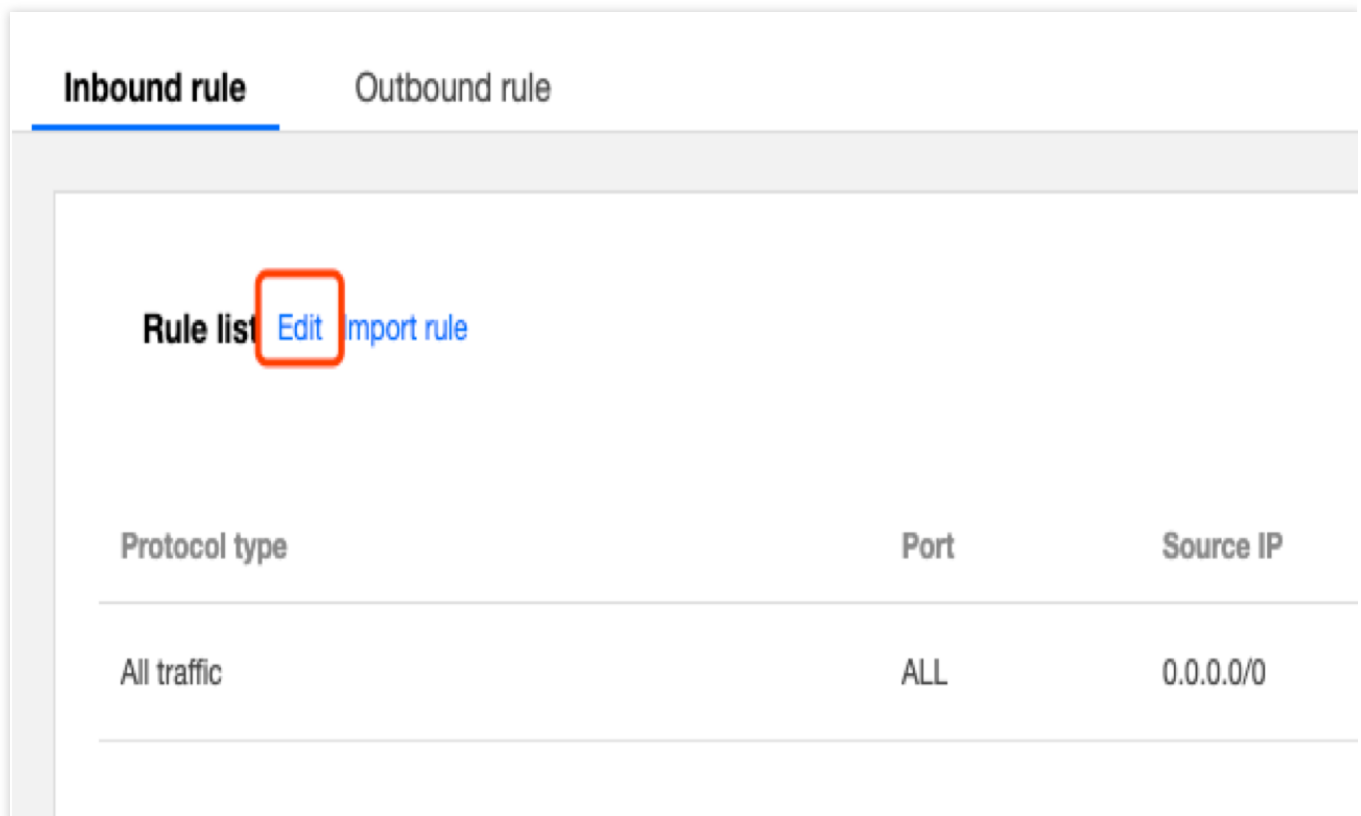
Protocol type	Port	Source IP	Policy	Notes
all	ALL	0.0.0.0/0	Refuse	

Below the table, there is a '+ New Line' button. At the bottom of the page, there are 'Save' and 'Cancel' buttons.

5. Click **Save**.

Deleting Network ACL Rules

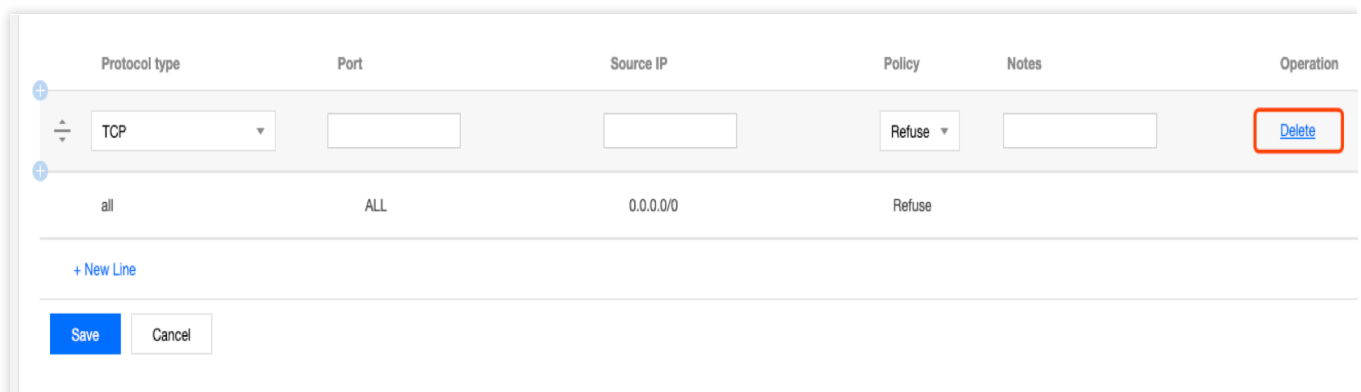
1. Log in to the [VPC console](#).
2. Click **Security** -> **Network ACL** in the directory on the left to go to the management page.
3. Look in the list for the network ACL to be deleted, and click its ID to go to the **Basic Information** page.
4. Click the **Inbound Rules** tab or the **Outbound Rules** tab to go to the **Rules List** page.
5. Click **Edit**. The process for deleting inbound rules is the same as for deleting outbound rules. The deletion of inbound rules is used as the example here.



6. In the list, select the row of the rule to be deleted and click **Delete** in the operation column.

Note:

This ACL rule is now grayed out. If you deleted it by accident, you can click **Recover the deleted rule** in the operation column to restore the rule.



7. Click **Save** to save the previous operation.

Note:

The deletion or restoration of the ACL rule only takes effect after you save the operation.

Associating Network ACLs with Subnets

1. Log in to the [VPC console](#).

2. Click **Security** -> **Network ACL** in the directory on the left to go to the management page.
3. Look in the list for the network ACL to be associated, and click its ID to go to the details page.
4. On the **Basic Information** page, click **Add Association** in the **Associated Subnets** module.

Bind Subnets

+ Bind

Batch unbind

<input type="checkbox"/>	Subnet name	Subnet ID

Selected 0 items, Total 0 items

5. Select the subnet to be associated from the pop-up window and click **OK**.

Bind Subnets ×

Select the subnet to be associated

Q

<input type="checkbox"/>	Subnet ID/name	Associated ACL	CIDR
<input type="checkbox"/>	subnet-368scdxa test2	-	192.168.0.0/24

OK Cancel

Disassociating Network ACLs from Subnets

1. Log in to the [VPC console](#).
2. Click **Security** -> **Network ACL** in the directory on the left to go to the management page.
3. Look in the list for the network ACL to be disassociated, and click its ID to go to the details page.
4. There are different methods for disassociating ACLs from subnets:

Method 1: look for the subnet that is to be disassociated in the **Associated Subnets** module on the **Basic Information** page and click **Disassociate**.

Bind Subnets

[+ Bind](#) [Batch unbind](#)

<input type="checkbox"/>	Subnet name	Subnet ID	CIDR	Operation
<input type="checkbox"/>	test2	subnet-368scdxa	192.168.0.0/24	Unbind

Selected 0 items, Total 1 items

Method 2: place a check next to the subnets that are to be disassociated in the **Associated Subnets** module on the **Basic Information** page, and click **Batch Disassociate**.

Bind Subnets

[+ Bind](#) [Batch unbind](#)

<input checked="" type="checkbox"/>	Subnet name	Subnet ID	CIDR
<input checked="" type="checkbox"/>	test2	subnet-368scdxa	192.168.0.0/24
<input checked="" type="checkbox"/>	aa	subnet-mc4zfl32	192.168.2.0/24

Selected 2 items, Total 2 items

5. Click **OK** in the pop-up window.

Bind Subnets

[+ Bind](#) [Batch unbind](#)

<input type="checkbox"/>	Subnet name	Subnet ID	CIDR	Operat
<input type="checkbox"/>	test2	subnet-368scdxa	192.168.0.0/24	Unbind
<input type="checkbox"/>	aa	subnet-mc4zfl32	192.168.2.0/24	

Selected 0 items, Total 2 items

Confirm to unbind the subnet?

[OK](#) [Cancel](#)

Deleting Network ACLs

1. Log in to the [VPC console](#).

- 2. Click **Security** -> **Network ACL** in the directory on the left to go to the management page.
- 3. Select the region and the VPC.
- 4. In the list, look for the network ACL to be deleted, click **Delete**, and then confirm the deletion. The network ACL and all of its rules will be deleted.

Note:

If the **Delete** option is grayed out, such as for the network ACL `testEg` in the following figure, it indicates that the network ACL is currently associated with a subnet. You will need to disassociate it from the subnet first before you can delete it.

+ New

Enter an ACL name or VPC

ID/Name	Associated subnets	Network	Operation
acl- test1<s>111	0	vpc-	Associated Subnets Delete
acl- testEg	1	vpc-	Associated Subnets Delete

Parameter Template

Overview

Last updated : 2024-10-22 16:14:58

A parameter template is a set of IP address or protocol port parameters. You can save IP addresses or protocol ports with the same needs as a template so that you can directly import the template as the source/destination IP or protocol port when adding security group rules. Parameter templates, if properly used, can enhance your efficiency in using security groups.

Use Cases

Parameter templates are mainly suitable for the following scenarios:

Manage multiple IP addresses or protocol port groups with the same requirements.

Manage multiple IP addresses or protocol port groups with frequent editing needs.

Parameter Template Types

Tencent Cloud supports the following four types of parameter templates:

IP address: also known as an IP address object, this template is a set of IP addresses and supports one single IP, CIDR block, and IP range.

IP address group: also known as an IP address group object, this template is a set of multiple IP address objects.

Protocol port: also known as a protocol port object, this template is a set of protocol ports and supports one single port, multiple ports, port range, and all ports. It supports TCP, UDP, ICMP, and GRE protocols.

Protocol port group: also known as a protocol port group object, this template is a set of protocol port objects.

Limits

Last updated : 2024-10-22 16:15:14

Use Limits

Formats supported by the IP address template are as follows:

Single IP address: such as 10.0.0.1 ;

Consecutive IP addresses: such as 10.0.0.1 - 10.0.0.100 ;

IP range: such as 10.0.1.0/24 .

Formats supported by the port template are as follows:

Single port: such as TCP:80 ;

Multiple ports: such as TCP:80,443 ;

Port range: such as TCP:3306-20000 ;

All ports: such as TCP:ALL .

Quota Limits

Instance	Upper Limit
IP address objects (ipm)	1,000 per tenant
IP address group objects (ipmg)	1,000 per tenant
Protocol port objects (ppm)	1,000 per tenant
Protocol port group objects (ppmg)	1,000 per tenant
IP address members in an IP address object (ipm)	20 per tenant
IP address object members (ipm) in an IP address group object (ipmg)	20 per tenant
Protocol port members in a protocol port group object (ppm)	20 per tenant
Protocol port object members (ppm) in a protocol port group object (ppmg)	20 per tenant
IP address group objects (ipmg) that can reference the same IP address object (ipm)	50 per tenant
Protocol port group objects (ppmg) that can reference the same protocol port object (ppm)	50 per tenant

Note:

If the parameter template is referenced by a security group, the IPs and ports in the template will be converted to multiple security group rules (up to 2000).

Managing Parameter Templates

Last updated : 2024-10-22 16:15:33

This document describes how to create and maintain parameter templates (IP address, IP address group, protocol port, and protocol port group) in the console and how to use them in security groups.

Creating a Parameter Template

Creating an IP Parameter Template

Add the IPs with the same usage or need to be edited frequently to the template.

Directions

1. Log in to the [VPC console](#).
2. Click **Security > Parameter Template** on the left sidebar to access the management page.
3. Select the **IP Address** tab and click **+ New**.
4. In the pop-up window, enter the name and IP addresses and click **Submit**.

You can add multiple IPs in the following ranges and separate them by line breaks:

Single IP: Such as "10.0.0.1" or "FF05::B5"

CIDR block: Such as "10.0.1.0/24" or "FF05:B5::/60"

Consecutive IPs: Such as `10.0.0.1 - 10.0.0.100` ;

Edit IP address

Name

test

IP address

1 153.222.104.108

2 88.132.67.65

3 104.57.124.183

4 153.10.125.102

5 14.71.34.15

6 21.95.127.91

7 156.140.73.12

8 136.66.172.192

9 172.17.177.94

10 172.17.235.139

11 172.17.24.116

12 172.17.14.106

13 172.17.88.58

14 172.17.83.236

15 172.17.182.21

16 172.17.27.38

Separated by line breaks. Supported formats: 10.0.0.1, 10.0.1.0/24, 10.0.0.1-10.0.0.100

Submit

Cancel

Creating an IP Group Template

You can add multiple addresses to an IP group for easy management.

Directions

1. Select the **IP Address Group** tab and click **+ New**.

Parameter Templates

IP address

IP address group

Protocol port

Protocol port group

+ New

2. In the pop-up window, enter the name, select the addresses to add, and click **Submit**.

✕

Edit IP address group

Name

test

Please select the IP address

Enter keyword

Q

☒ ipm-j7uiaxq6
test2

☒ ipm-pg17kvte
dongyuan

Selected(2)

ipm-j7uiaxq6
test2

✕

ipm-pg17kvte
dongyuan

✕

↔

Submit

Cancel

Creating a Protocol + Port Group Template

Create a template and add combinations of protocol and port to it for easy management.

Directions

1. Log in to the [VPC console](#).
2. Click **Security > Parameter Template** on the left sidebar to access the management page.
3. Select the **Protocol Port** tab and click **+ New**.
4. In the pop-up window, enter the name and protocol ports and click **Submit**.

You can add multiple protocol ports in the following ranges and separate them with line breaks:

Single port: Such as TCP:80 ;

Multiple ports: Such as TCP:80,443 ;

Port range: Such as TCP:3306-20000 ;

All ports: TCP:ALL .

Create Protocol port

Name

test

Protocol

port

1 TCP:80

2 TCP:443

Separated by line breaks. Supported formats: TCP:80, TCP:80,443, TCP:3306-20000, TCP:All

Submit

Cancel

Creating protocol port group parameter template

You can add multiple created protocol port objects to a protocol port group for unified management.

Directions

1. Select the **Protocol Port Group** tab and click **+ New**.

Parameter Templates

IP address

IP address group

Protocol port

Protocol port group


+ New

2. In the pop-up window, enter the name, select the protocol port object to be added, and click **Submit**.

Create Protocol port group

Name


Please select the protocol port


Enter keyword 

☒ ppm-hdby5uu0
test2

☐ ppm-6dp3nfv4
test

Selected(1)

ppm-hdby5uu0
test2 



Submit

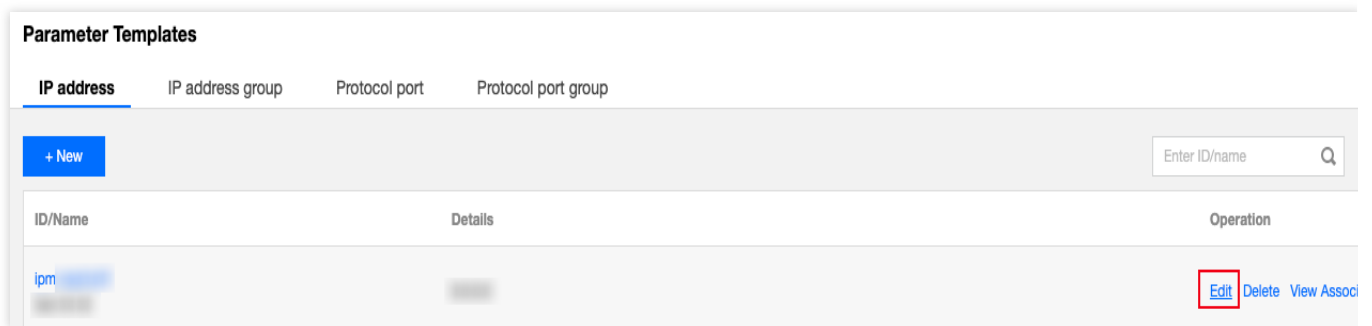
Cancel

Modifying a Parameter Template

If you need to modify a created parameter template, for example, to add/delete IP addresses or protocol ports, follow the steps below.

Directions

1. Click the created IP address, IP address group, protocol port, or protocol port group parameter template and click **Edit** on the right.



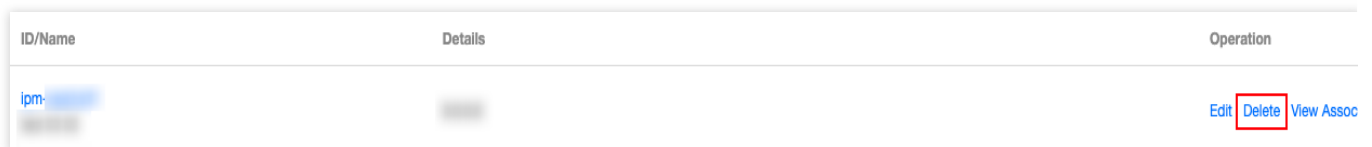
2. In the pop-up window, modify the corresponding parameters and click **Submit**.

Deleting a Parameter Template

When a template is deleted, all the policy configurations containing it in the security group will be deleted at the same time. Please evaluate and proceed with caution.

Directions

1. Click **Delete** on the right of the template.



2. When this template is deleted, all the policies containing the corresponding IP address or protocol port will also be deleted. After confirming that everything is correct, click **Delete** in the **Confirm Deletion** pop-up window.

Referring the Template in a Security Group

When you add a security group rule, you can refer to the templates to add IPs and ports quickly.

Directions

1. Log in to the [VPC console](#).
2. Click **Security > Security Group** on the left sidebar to access the management page.
3. In the list, find the target security group and click its ID to enter the details page.
4. On the **Inbound/Outbound Rules** tab, click **Add Rule**.
5. In the pop-up window, select the **Custom** type, select the created parameter template in **Source** and **Protocol Port**, and click **Complete**. For more information on how to add inbound/outbound rules, please see [Adding a Security Group Rule](#).

Note

If you need to add a new IP address or protocol port in the future, you only need to add it to the corresponding IP address group or protocol port group, and there is no need to modify the security group rules or create another security group.

Add Inbound rule

Type	Source ⓘ	Protocol port ⓘ	Policy	Notes	
Custom ▾	For example, 10.0.0.1 or 10	For example, UDP:53, TCP:80/443 or T	Allow ▾		Delete
+ New Line					

Completed

Cancel

Viewing Associated Security Group

You can view all security group instances that import a parameter template in the following steps.

1. Click **View Association** on the right of the created parameter template.

ID/Name	Details	Operation
ipm- <div></div>	<div></div>	Edit Delete View Associ

2. The associated security group list that pops up displays all security group instances associated with this parameter template.

Query Associated Security Groups

ID	Name	Category
sg- <div></div>	<div></div>	Security Groups

Close

Importing a Parameter Template

To batch add parameter template configurations, do the following:

1. Click **Import** on the right of the created parameter template.
2. Upload a local file.

Exporting a Parameter Template

To back up the parameter templates to local, click **Export** on the right of the created parameter template.

Configuration Case

Last updated : 2024-10-22 16:15:50

Parameter Template Use Cases

Parameter template is an efficient, fast, and easy-to-maintain way to add rules in security groups. For example, when you need to add multiple IP ranges, specified IPs, or protocol ports of multiple types, you can define a parameter template. You can also use the parameter template subsequently to maintain the IP sources and protocol ports in the security group rules.

Note:

All the IP addresses and protocol ports in this document are examples. Please replace them according to your actual business conditions during configuration.

Example Description

Suppose you want to configure the following security group rules and need to update the inbound source IP range and protocol port later:

Inbound rules:

Allowed source IP range: 10.0.0.16-10.0.0.30; protocol port: TCP:80,443

Allowed source CIDR block: 192.168.3.0/24; protocol port: TCP:3600-15000

Outbound rules:

Rejected target IP address: 192.168.10.4; protocol port: TCP:800

Solution

Because you have the same security group policy for multiple IP ranges and protocol ports, and you need to update the source IP range later, you can use a parameter template to implement the addition and maintenance of security group rules.

Step 1. Create a parameter template

1. Log in to the [VPC console](#).
2. Select **Security > Parameter Template** on the left sidebar to access the management page.
3. On the **IP Address** tab, click **+ New** to create an IP address parameter template for adding inbound and outbound rules.
4. In the pop-up window, enter the source IP range and click **Submit**.

Create IP address

Name

test

IP address

1 10.0.0.1

2 10.0.1.0/24

3 10.0.0.1-10.0.0.100

4

Separated by line breaks. Supported formats: 10.0.0.1, 10.0.1.0/24, 10.0.0.1-10.0.0.100

Submit

Cancel

The newly created IP address parameter template is as shown below.

Parameter Templates		
IP address		
+ New		
ID/Name	Details	Operation
ipm-		Edit Delete View Associa
ipm-		Edit Delete View Associa

5. On the **Protocol Port** tab, click **+ New** to create a protocol port parameter template for adding inbound and outbound rules.

Create Protocol port

Name

test

Protocol

port

1 TCP:80

Separated by line breaks. Supported formats: TCP:80, TCP:80,443, TCP:3306-20000, TCP:All

Submit

Cancel

The newly created protocol port parameter template is as shown below:

Parameter Templates

IP address IP address group **Protocol port** Protocol port group

[+ New](#) [Q](#) [↻](#)

ID/Name	Details	Operation
ppm- [blurred]	tcp: [blurred]	Edit Delete View Associatio
ppm- [blurred]	tcp: [blurred]	Edit Delete View Associatio

Step 2. Add a security group rule

1. Log in to the [VPC console](#).
2. Select **Security** > **Security Group** on the left sidebar to access the management page.
3. In the list, find the security group that needs to import the parameter template and click its ID to enter the details page.
4. On the **Inbound/Outbound Rules** tab, click **Add Rule**.
5. In the pop-up window, select the custom type, select the corresponding IP address parameter template for the source/target, select the corresponding protocol port parameter template for the protocol port, and click **Complete**.

Add inbound rule

Type	Source ⓘ	Protocol Port ⓘ	Policy	Notes
Custom ▼	ipm-[blurred]	ppm-[blurred]	Allow ▼	
+New Line				
Complete Cancel				

Step 3. Update the parameter template

Suppose you need to add an inbound rule with the IP source being the `10.0.1.0/27` IP range and the protocol port being `UDP:58`. You can directly update the parameter templates of the IP address `ipm-0ge3ob8e` and the protocol port `ppm-4ty1ck3i`.

1. On the **IP Address** tab of the parameter template, find the `ipm-0ge3ob8e` parameter template.
2. Click **Edit** on the right.

Parameter Templates

IP address IP address group Protocol port Protocol port group

+ New

Enter ID/name

ID/Name	Details	Operation
ipm-		Edit Delete View Associati

3. In the pop-up window, add the `10.0.1.0/27` IP range in a new line and click **Submit**.

Edit IP address

Name

IP address

1

8.

2

10.0.1.0/27

Separated by line breaks. Supported formats: 10.0.0.1, 10.0.1.0/24, 10.0.0.1-10.0.0.100

Submit **Cancel**

4. On the **Protocol Port** tab of the parameter template, find the `ppm-4ty1ck3i` parameter template.

5. Click **Edit** on the right.

Parameter Templates

IP address

IP address group

Protocol port

Protocol port group

+ New

Enter ID/name



ID/Name

Details

Operation

ppm-

[Edit](#)[Delete](#)[View Associat](#)

6. In the pop-up window, add the `UDP : 58` inbound protocol port in a new line and click **Submit**.

Edit Protocol port



Name

Protocol

port

```
1 tcp:
2 UDP:58
```

Separated by line breaks. Supported formats: TCP:80, TCP:80,443, TCP:3306-20000, TCP:All

Submit

Cancel

Access Management

Cloud Access Management Overview

Last updated : 2024-10-22 16:16:08

If you are using multiple Tencent Cloud services such as VPC, CVM, and TencentDB that are managed by different users sharing your Tencent Cloud account key, you may encounter the following problems:

Your key is shared by multiple users, which poses a high risk of leakage.

You cannot limit the access permissions of other users, which poses a security risk due to potential misoperation.

To prevent these problems, you can use sub-accounts to allow different users to manage different services. By default, a sub-account has no permission to use a CVM or CVM-related resources. Therefore, you need to create a policy to grant the required resources or permissions to sub-accounts.

Overview

Cloud Access Management (CAM) is a web service provided by Tencent Cloud to help customers manage the permissions to access resources under their Tencent Cloud accounts in a secure way. You can use CAM to create, manage, and terminate users (or user groups), and use identity management and policy management to control Tencent Cloud resources that can be used by each user.

When using CAM, you can associate a policy to a user or a group of users. The policy can authorize or deny users' requests of using specified resources to complete specified tasks.

For more basic information on CAM policies, see [Syntax Logic](#).

For more usage information on CAM policies, see [Policies](#).

If you do not need to manage the access permissions of sub-accounts for VPC resources, you can skip this section. This will not affect your understanding and usage of other parts in the document.

Getting Started

A CAM policy must authorize or deny the use of one or more VPC operations. At the same time, it must specify the resources (which can be all resources or partial resources for certain operations) that can be used for the operations. The policy can also include the conditions set for the operation resources.

Some VPC API operations support resource-level permissions. That is, when calling these APIs, you cannot specify some resources for the operations. Instead, you must specify all resources for the operations.

Task	Link
Basic structure of a policy	Policy Syntax

Define operations in the policy	VPC Operations
Define resources in the policy	VPC Resource Paths
Resource-level permissions supported by VPC	Resource-Level Permissions Supported by VPC
Console example	Console Example

Authorizable Resource Types

Last updated : 2024-10-22 16:16:26

Policy Syntax

CAM policy:

```
{
  "version": "2.0",
  "statement": [
    {
      "effect": "effect",
      "action": ["action"],
      "resource": ["resource"],
      "condition": {"key": {"value"}}
    }
  ]
}
```

version is required. Currently, only the "2.0" value is allowed.

statement describes the details of one or more permissions. This element contains a permission or permission set of other elements such as effect, action, resource, and condition. Each policy has one statement element.

1.1 **action** describes the action to be allowed or denied. An action can be an API (described using the prefix "name") or a feature set (a set of specific APIs described with the prefix "permid"). This element is required.

1.2 **resource** describes the details of authorization. A resource is described in a six-piece format. Detailed resource definitions vary by product. For more information on how to specify a resource, see the documentation for the product whose resources you are writing a statement for. This element is required.

1.3 **condition** describes the condition for the policy to take effect. A condition consists of an operator, an action key, and an action value. A condition value may contain information such as the time and IP address. Some services allow you to specify additional values in a condition. This element is optional.

1.4 **effect** describes whether the result produced by the statement is "allow" or "deny". This element is required.

VPC Operations

In the statement of a CAM policy, you can specify any API action from any service that supports CAM. For VPC, use APIs with the prefix "name/vpc:", for example, name/vpc:Describe or name/vpc:CreateRoute.

To specify multiple actions in a single statement, separate them with commas, as shown below:

```
"action":["name/vpc:action1","name/vpc:action2"]
```

You can also specify multiple actions by using a wildcard. For example, you can specify all actions whose names begin with "Describe", as shown below:

```
"action":["name/vpc:Describe*"]
```

To specify all actions in VPC, use the wildcard "*" as follows:

```
"action": ["name/vpc:*"]
```

VPC Resource Paths

Each CAM policy statement has its own resources.

The general format of a resource path is as follows:

```
****qcs*:project_id:service_type:region:account:resource**
```

project_id: project information. This element is only used to enable compatibility with legacy CAM logic and can be left empty.

service_type: the product abbreviation, such as VPC.

region: region information, such as bj.

account: the root account of the resource owner, such as uin/164256472.

resource: resource details of each product, such as vpc/vpc_id1 or vpc/*.

For example, you can specify an instance (vpc-d08sl2zr in this case) in the statement, as shown below:

```
"resource": [ "qcs::vpc:bj:uin/164256472:instance/vpc-d08sl2zr" ]
```

You can also use the wildcard "*" to specify all instances under a specific account, as shown below:

```
"resource": [ "qcs::vpc:bj:uin/164256472:instance/*" ]
```

To specify all resources or if any API action does not support resource-level permissions, you can use the wildcard "*" in the Resource element, as shown below:

```
"resource": [ "*" ]
```

To specify multiple resources in one instruction, separate them with commas. In the following example, two resources are specified:

```
"resource": ["resource1", "resource2"]
```

The following table describes the resources that can be used by VPC and the corresponding methods of describing these resources.

In the following table, the words prefixed with "\$" are all alternative names.

`project` indicates the project ID.

`region` indicates the region.

`account` indicates the account ID.

Resource	Resource Description Method in the Authorization Policy
VPC	<code>qcs::vpc:\$region:\$account:vpc/\$vpclId</code>
Subnet	<code>qcs::vpc:\$region:\$account:subnet/\$subnetId</code>
Security group	<code>qcs::cvm:\$region:\$account:sg/\$sgId</code>
EIP	<code>qcs::cvm:\$region:\$account:eip/*</code>

VPC Access Management Policy Examples

Last updated : 2024-10-22 16:16:43

Full Read-Write Policy of VPC

The following policy allows you to create and manage VPC instances. You can associate this policy with a group of network admins. The Action element specifies all VPC-related APIs.

```
{
  "version": "2.0",
  "statement": [
    {
      "action": [
        "name/vpc:*"
      ],
      "resource": "*",
      "effect": "allow"
    }
  ]
}
```

Read-only Policy of VPC

The following policy allows you to query your VPC instances and relevant resources. However, you cannot create, update, or delete them with this policy.

We recommend that you grant the VPC read-only permission for users, because they have to be able to view the resource in order to operate it in the console.

```
{
  "version": "2.0",
  "statement": [
    {
      "action": [
        "name/vpc:Describe*",
        "name/vpc:Inquiry*",
        "name/vpc:Get*"
      ],
      "resource": "*",
      "effect": "allow"
    }
  ]
}
```

```
]
}
```

Allowing a Sub-Account to Manage Only a Single VPC

The following policy allows a user to view all VPC instances but only to be able to operate VPC A (for example, VPC A with an ID of vpc-d08sl2zr) and network resources in VPC A (such as subnets and route tables, but excluding cloud virtual machines (CVMs) and databases). In other words, the user is not allowed to manage other VPC instances.

This version does not support **allowing the user to see A only**, which however will be supported in future versions.

```
{
  "version": "2.0",
  "statement": [
    {
      "action": "name/vpc:*",
      "resource": "*",
      "effect": "allow",
      "condition": {
        "string_equal_if_exist": {
          "vpc:vpc": [
            "vpc-d08sl2zr"
          ],
          "vpc:accepter_vpc": [
            "vpc-d08sl2zr"
          ],
          "vpc:requester_vpc": [
            "vpc-d08sl2zr"
          ]
        }
      }
    }
  ]
}
```

Allowing a User to Manage VPC Instances But Not Operate Route Tables

The following policy allows a user to read and write VPC instances and relevant resources, but disallows the user to operate route tables.

```
{
  "version": "2.0",
  "statement": [
    {
      "action": [
        "name/vpc:*"
      ],
      "resource": "*",
      "effect": "allow"
    },
    {
      "action": [
        "name/vpc:AssociateRouteTable",
        "name/vpc:CreateRoute",
        "name/vpc:CreateRouteTable",
        "name/vpc>DeleteRoute",
        "name/vpc>DeleteRouteTable",
        "name/vpc:ModifyRouteTableAttribute"
      ],
      "resource": "*",
      "effect": "deny"
    }
  ]
}
```

Allowing a User to Manage VPN Resources

The following policy allows a user to view all VPC resources, while only allows the user to create, read, update, and delete (CRUD) the resources on VPNs.

```
{
  "version": "2.0",
  "statement": [
    {
      "action": [
        "name/vpc:Describe*",
        "name/vpc:Inquiry*",
        "name/vpc:Get*"
      ],
      "resource": "*",
      "effect": "allow"
    },
    {
```

```
        "action": [
            "name/vpc:*Vpn*",
            "name/vpc:*UserGw*"
        ],
        "resource": "*",
        "effect": "allow"
    }
]
```

Resource-Level Permissions Supported by VPC APIs

Last updated : 2024-10-22 16:17:05

You can authorize the following API operations for VPC resources in CAM. Resources supported by specific APIs and the corresponding conditions are as follows:

Note :

Any VPC API operation that is not listed in the table does not support resource-level permissions. For such an operation, you can still authorize a user to perform it, but you must specify * as the resource element in the policy statement.

Configuring using API	Resources
AcceptVpcPeeringConnection	VPC resource qcs::vpc:\$region:\$account:vpc/* qcs::vpc:\$region:\$account:vpc/\$vpcId
—	Peering connection resource qcs::vpc:\$region:\$account:pcx/* qcs::vpc:\$region:\$account:pcx/\$peeringConnectionId
—	VPC resource qcs::vpc:\$region:\$account:vpc/* qcs::vpc:\$region:\$account:vpc/\$vpcId (the receiver's vpcId)
AcceptVpcPeeringConnectionEx	Peering connection resource qcs::vpc:\$region:\$account:pcx/* qcs::vpc:\$region:\$account:pcx/\$peeringConnectionId
—	VPC resource

	qcs::vpc:\$region:\$account:vpc/* qcs::vpc:\$region:\$account:vpc/\$vpcId
AddVpnConnEx	VPC resource qcs::vpc:\$region:\$account:vpc/* qcs::vpc:\$region:\$account:vpc/\$vpcId
—	VPN gateway resource qcs::vpc:\$region:\$account:vpngw/* qcs::vpc:\$region:\$account:vpngw/\$vpnGwId
—	Customer gateway resource qcs::vpc:\$region:\$account:cgw/*
—	VPN tunnel resource qcs::vpc:\$region:\$account:vpn/*
AssignPrivateIpAddresses	ENI resource qcs::vpc:\$region:\$account:eni/* qcs::vpc:\$region:\$account:eni/\$networkInterfaceId
AssociateRouteTable	Subnet resource qcs::vpc:\$region:\$account:subnet/* qcs::vpc:\$region:\$account:subnet/\$subnetId
—	Route table resource qcs::vpc:\$region:\$account:rtb/* qcs::vpc:\$region:\$account:rtb/\$routeTableId
AttachClassicLinkVpc	VPC resource qcs::vpc:\$region:\$account:vpc/* qcs::vpc:\$region:\$account:vpc/\$vpcId
—	CVM resource

	qcs::cvm:\$region:\$account:instance/* qcs::cvm:\$region:\$account:instance/\$instanceId
AttachNetworkInterface	ENI resource qcs::vpc:\$region:\$account:eni/* qcs::vpc:\$region:\$account:eni/\$networkInterfaceId
—	CVM resource qcs::cvm:\$region:\$account:instance/* qcs::cvm:\$region:\$account:instance/\$instanceId
CreateAndAttachNetworkInterface	VPC resource qcs::vpc:\$region:\$account:vpc/* qcs::vpc:\$region:\$account:vpc/\$vpcId
—	CVM resource qcs::cvm:\$region:\$account:instance/* qcs::cvm:\$region:\$account:instance/\$instanceId
—	ENI resource qcs::vpc:\$region:\$account:eni/*
CreateDirectConnectGateway	VPC resource qcs::vpc:\$region:\$account:vpc/* qcs::vpc:\$region:\$account:vpc/\$vpcId
—	Direct connect gateway resource qcs::vpc:\$region:\$account:dcg/*
CreateLocalDestinationIPPortTranslationNatRule	Direct connect gateway resource qcs::vpc:\$region:\$account:dcg/* qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId
CreateLocalIPTranslationAclRule	Direct connect gateway resource qcs::vpc:\$region:\$account:dcg/* qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId

CreateLocalIPTranslationNatRule	Direct connect gateway resource qcs::vpc:\$region:\$account:dcg/* qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId
CreateLocalSourceIPPortTranslationAclRule	Direct connect gateway resource qcs::vpc:\$region:\$account:dcg/* qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId
CreateLocalSourceIPPortTranslationNatRule	Direct connect gateway resource qcs::vpc:\$region:\$account:dcg/* qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId
CreatePeerIPTranslationNatRule	Direct connect gateway resource qcs::vpc:\$region:\$account:dcg/* qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId
CreateNatGateway	VPC resource qcs::vpc:\$region:\$account:vpc/* qcs::vpc:\$region:\$account:vpc/\$vpcId
—	NAT gateway resource qcs::vpc:\$region:\$account:nat/*
CreateNetworkAcl	VPC resource qcs::vpc:\$region:\$account:vpc/* qcs::vpc:\$region:\$account:vpc/\$vpcId
—	Network ACL resource qcs::vpc:\$region:\$account:acl/*
CreateNetworkInterface	VPC resource qcs::vpc:\$region:\$account:vpc/* qcs::vpc:\$region:\$account:vpc/\$vpcId
—	Subnet resource qcs::vpc:\$region:\$account:subnet/* qcs::vpc:\$region:\$account:subnet/\$subnetId

—	ENI resource qcs::vpc:\$region:\$account:eni/*
CreateRoute	Route table resource qcs::vpc:\$region:\$account:rtb/* qcs::vpc:\$region:\$account:rtb/\$routeTableId
CreateRouteTable	VPC resource qcs::vpc:\$region:\$account:vpc/* qcs::vpc:\$region:\$account:vpc/\$vpcId
—	Route table resource qcs::vpc:\$region:\$account:rtb/*
CreateSubnet	VPC resource qcs::vpc:\$region:\$account:vpc/* qcs::vpc:\$region:\$account:vpc/\$vpcId
—	Subnet gateway resource qcs::vpc:\$region:\$account:subnet/*
CreateSubnetAclRule	Network ACL resource qcs::vpc:\$region:\$account:acl/* qcs::vpc:\$region:\$account:acl/\$networkAclId
—	Subnet gateway resource qcs::vpc:\$region:\$account:subnet/*
CreateVpcPeeringConnection	VPC resource (initiator) qcs::vpc:\$region:\$account:vpc/*

	qcs::vpc:\$region:\$account:vpc/\$vpcId
—	Peering connection resource qcs::vpc:\$region:\$account:pcx/*
CreateVpcPeeringConnectionEx	VPC resource qcs::vpc:\$region:\$account:vpc/* qcs::vpc:\$region:\$account:vpc/\$vpcId
—	Peering connection resource qcs::vpc:\$region:\$account:pcx/*
DeleteDirectConnectGateway	Direct connect gateway resource qcs::vpc:\$region:\$account:dcg/* qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId
DeleteLocalDestinationIPPortTranslationNatRule	Direct connect gateway resource qcs::vpc:\$region:\$account:dcg/* qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId
DeleteLocalIPTranslationAclRule	Direct connect gateway resource qcs::vpc:\$region:\$account:dcg/* qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId
DeleteLocalIPTranslationNatRule	Direct connect gateway resource qcs::vpc:\$region:\$account:dcg/* qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId

DeleteLocalSourceIPPortTranslationAclRule	Direct connect gateway resource qcs::vpc:\$region:\$account:dcg/* qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId
DeletePeerIPTTranslationNatRule	Direct connect gateway resource qcs::vpc:\$region:\$account:dcg/* qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId
DeleteLocalSourceIPPortTranslationNatRule	Direct connect gateway resource qcs::vpc:\$region:\$account:dcg/* qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId
DeleteNatGateway	NAT gateway resource qcs::vpc:\$region:\$account:nat/* qcs::vpc:\$region:\$account:nat/\$natId
DeleteNetworkAcl	Network ACL resource qcs::vpc:\$region:\$account:acl/* qcs::vpc:\$region:\$account:acl/\$networkAclId
DeleteNetworkInterface	ENI resource qcs::vpc:\$region:\$account:eni/* qcs::vpc:\$region:\$account:eni/\$networkInterfaceId
DeleteRoute	Route table resource qcs::vpc:\$region:\$account:rtb/* qcs::vpc:\$region:\$account:rtb/\$routeTableId
DeleteRouteTable	Route table resource qcs::vpc:\$region:\$account:rtb/* qcs::vpc:\$region:\$account:rtb/\$routeTableId
DeleteSubnet	Subnet resource qcs::vpc:\$region:\$account:subnet/* qcs::vpc:\$region:\$account:subnet/\$subnetId

DeleteUserGw	Customer gateway resource qcs::vpc:\$region:\$account:cgw/* qcs::vpc:\$region:\$account:cgw/\$userGwId
DeleteVpc	VPC resource qcs::vpc:\$region:\$account:vpc/* qcs::vpc:\$region:\$account:vpc/\$vpcId
DeleteVpcPeeringConnection	Peering connection resource qcs::vpc:\$region:\$account:pcx/* qcs::vpc:\$region:\$account:pcx/\$peeringConnectionId
DeleteVpcPeeringConnectionEx	Peering connection resource qcs::vpc:\$region:\$account:pcx/* qcs::vpc:\$region:\$account:pcx/\$peeringConnectionId
DeleteVpnConn	VPN tunnel resource qcs::vpc:\$region:\$account:vpn/*qcs::vpc:\$region:\$account:vpn/\$vpnId
DetachClassicLinkVpc	VPC resource qcs::vpc:\$region:\$account:vpc/* qcs::vpc:\$region:\$account:vpc/\$vpcId
—	CVM resource qcs::cvm:\$region:\$account:instance/*qcs::cvm:\$region:\$account:instance/\$instanceId

DetachNetworkInterface	CVM resource qcs::cvm:\$region:\$account:instance/*qcs::cvm:\$region:\$account:instance/*
—	ENI resource qcs::vpc:\$region:\$account:eni/* qcs::vpc:\$region:\$account:eni/\$networkInterfaceId
DeleteSubnetACLRule	Subnet resource qcs::vpc:\$region:\$account:subnet/* qcs::vpc:\$region:\$account:subnet/\$subnetId
—	Network ACL resource qcs::vpc:\$region:\$account:acl/* qcs::vpc:\$region:\$account:acl/\$networkAclId
EipBindNatGateway	NAT gateway resource qcs::vpc:\$region:\$account:nat/* qcs::vpc:\$region:\$account:nat/\$natId
EipUnBindNatGateway	NAT gateway resource qcs::vpc:\$region:\$account:nat/* qcs::vpc:\$region:\$account:nat/\$natId
EnableVpcPeeringConnection	VPC resource qcs::vpc:\$region:\$account:vpc/* qcs::vpc:\$region:\$account:vpc/\$vpcId
—	Peering connection resource qcs::vpc:\$region:\$account:pcx/* qcs::vpc:\$region:\$account:pcx/\$peeringConnectionId
EnableVpcPeeringConnectionEx	VPC resource qcs::vpc:\$region:\$account:vpc/* qcs::vpc:\$region:\$account:vpc/\$vpcId

—	Peering connection resource qcs::vpc:\$region:\$account:pcx/* qcs::vpc:\$region:\$account:pcx/\$peeringConnectionId
MigrateNetworkInterface	ENI resource qcs::vpc:\$region:\$account:eni/* qcs::vpc:\$region:\$account:eni/\$networkInterfaceId
—	CVM Resource qcs::cvm:\$region:\$account:instance/*qcs::cvm:\$region:\$account:instance/* (permission is required before and after the migration)
MigratePrivateIpAddress	ENI resource qcs::vpc:\$region:\$account:eni/* qcs::vpc:\$region:\$account:eni/\$networkInterfaceId
ModifyDirectConnectGateway	Direct connect gateway resource qcs::vpc:\$region:\$account:dcg/* qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId
ModifyLocalDestinationIPPortTranslationNatRule	Direct connect gateway resource qcs::vpc:\$region:\$account:dcg/* qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId
ModifyLocalIPTranslationAclRule	Direct connect gateway resource qcs::vpc:\$region:\$account:dcg/* qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId

ModifyLocalIPTranslationNatRule	Direct connect gateway resource qcs::vpc:\$region:\$account:d qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId
ModifyLocalSourceIPPortTranslationAclRule	Direct connect gateway resource qcs::vpc:\$region:\$account:d qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId
ModifyPeerIPTranslationNatRule	Direct connect gateway resource qcs::vpc:\$region:\$account:d qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId
ModifyLocalSourceIPPortTranslationNatRule	Direct connect gateway resource qcs::vpc:\$region:\$account:d qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId
ModifyNatGateway	NAT gateway resource qcs::vpc:\$region:\$account:nat/* qcs::vpc:\$region:\$account:nat/nat-dc7cdf
ModifyNetworkAcl	Network ACL resource qcs::vpc:\$region:\$account:acl/* qcs::vpc:\$region:\$account:acl/\$networkAclId
ModifyNetworkAclEntry	Network ACL resource qcs::vpc:\$region:\$account:acl/* qcs::vpc:\$region:\$account:acl/\$networkAclId
ModifyNetworkInterface	ENI resource qcs::vpc:\$region:\$account:eni/* qcs::vpc:\$region:\$account:eni/\$networkInterfaceId
ModifyPrivateIpAddress	ENI resource qcs::vpc:\$region:\$account:eni/* qcs::vpc:\$region:\$account:eni/\$networkInterfaceId

ModifyRouteTableAttribute	Route table resource qcs::vpc:\$region:\$account:rtb/* qcs::vpc:\$region:\$account:rtb/\$routeTableId
ModifySubnetAttribute	Subnet resource qcs::vpc:\$region:\$account:subnet/* qcs::vpc:\$region:\$account:subnet/\$subnetId
ModifyUserGw	Customer gateway resource qcs::vpc:\$region:\$account:cgw/* qcs::vpc:\$region:\$account:cgw/\$userGwId
ModifyVpcAttribute	VPC resource qcs::vpc:\$region:\$account:vpc/* qcs::vpc:\$region:\$account:vpc/\$vpcId
ModifyVpcPeeringConnection	VPC resource qcs::vpc:\$region:\$account:vpc/* qcs::vpc:\$region:\$account:vpc/\$vpcId
—	Peering connection resource qcs::vpc:\$region:\$account:pcx/* qcs::vpc:\$region:\$account:pcx/\$peeringConnectionId
ModifyVpcPeeringConnectionEx	VPC resource qcs::vpc:\$region:\$account:vpc/* qcs::vpc:\$region:\$account:vpc/\$vpcId
—	Peering connection resource qcs::vpc:\$region:\$account:pcx/* qcs::vpc:\$region:\$account:pcx/\$peeringConnectionId

ModifyVpnConnEx	VPN tunnel resource qcs::vpc:\$region:\$account:vpn/* qcs::vpc:\$region:\$account:vpn/\$vpnConnId
ModifyVpnGw	VPN gateway resource qcs::vpc:\$region:\$account:vpngw/* qcs::vpc:\$region:\$account:vpngw/\$vpnGwId
RejectVpcPeeringConnection	VPC resource qcs::vpc:\$region:\$account:vpc/* qcs::vpc:\$region:\$account:vpc/\$vpcId
—	Peering connection resource qcs::vpc:\$region:\$account:pcx/* qcs::vpc:\$region:\$account:pcx/\$peeringConnectionId
RejectVpcPeeringConnectionEx	VPC resource qcs::vpc:\$region:\$account:vpc/* qcs::vpc:\$region:\$account:vpc/\$vpcId
—	Peering connection resource qcs::vpc:\$region:\$account:pcx/* qcs::vpc:\$region:\$account:pcx/\$peeringConnectionId
ResetVpnConnSA	VPN tunnel resource qcs::vpc:\$region:\$account:vpn/* qcs::vpc:\$region:\$account:vpn/\$vpnConnId

SetLocalIPTranslationAclRule	Direct connect gateway resource qcs::vpc:\$region:\$account:d qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId
SetLocalSourceIPPortTranslationAclRule	Direct connect gateway resource qcs::vpc:\$region:\$account:d qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId
SetSSLVpnDomain	VPN gateway resource qcs::vpc:\$region:\$account:vpngw/* qcs::vpc:\$region:\$account:vpngw/\$vpnGwId
UnassignPrivateIpAddresses	ENI resource qcs::vpc:\$region:\$account:eni/* qcs::vpc:\$region:\$account:eni/\$networkInterfaceId

Diagnostic Tools

Network Probe

Last updated : 2024-10-22 16:20:33

The Tencent Cloud network probe service is used to monitor the quality of VPC network connections, including latency, packet loss rate, and other key metrics.

Under the hybrid cloud network architecture, you create a network probe in the subnet that needs to communicate with your IDC to monitor the packet loss rate and latency of the probed linkage. The configuration allows you to:

Monitor the connection quality

Receive alerts in case of connection failures

Instructions

The network probe service adopts ping method with a frequency of 20 pings per minute.

Up to 50 probes are allowed for each VPC.

A maximum of 20 subnets under the same VPC can have network probes.

Creating a Network Probe

1. Log in to [VPC console](#).
2. Select **Diagnostic Tools** -> **Network Probe** in the left sidebar to enter the management page.
3. Click **+New** at the top of the **Network Probe** page.
4. In the **Create Network Probe** pop-up window, fill in relevant fields.

Note:

The network probe route is assigned by the system and cannot be modified.

When you switch the route of subnet, this default route will be removed from the original route table associated with the subnet, and be added to the new route table associated.

Create Network Probe

Name

Virtual Private Cloud

Please select...

Subnet

Please select...

i

Destination IP to probe

Enter the destination IP to probe, and verify it

Verify i

Optional

Verify

Next hop

NAT Gateway

No available NAT gatew

i

Statistical Method

Average

i

Notes

Create

Cancel

Field description

Field	Configuration
Name	Name of the network probe.
VPC	The VPC to which the probe source IP belongs.
Subnet	The subnet to which the probe source IP belongs.
Probe Destination IP	A maximum of two destination IPs are supported for the network probe. Please ensure that you've enabled ICMP firewall policy for the destination server of network probe.
Source Next Hop	You can choose to Specify or Do Not Specify the next hop. If Do Not Specify is chosen, no next hop will be selected. Note :

Do Not Specify is now only available to beta users. To enable it, please [submit a ticket](#).
If you specify the next hop, select the next hop type and instances. And then, the system automatically adds the corresponding 32-bit route to the subnet-associated route table.
Currently, the supported next hop type includes NAT Gateway, peering connections, VPN gateway, direct connect gateway, CVM(Public Gateway) , CVM, and CCN.

Note :

If you specify the CCN as the next hop and the probe destination IPs belong to two VPCs in the CCN, the IP range with the longest mask will be matched and take effect.

5. (Optional) **Verify** the **Probe Destination IP**.

Note:

Skip this step if you do not specify the next hop.

If the connection succeeds, click **OK**.

If the connection fails, check whether the subnet route is correctly configured, and whether the probed device enables Network ACL, security group or other firewalls, which may block the connection. For more information, see [Managing Network ACLs](#) and [Modifying a Security Group Rule](#).

Checking the Latency and Packet Loss of a Network Probe

1. Log in to [VPC console](#).
2. Select **Diagnostic Tools** > **Network Probe** in the left sidebar to enter the management page.
3. Click



of the target network probe instance to view its latency and packet loss rate.

+ New			
ID/Name	Monitoring	Virtual Private Cloud	Subnet
netd-ap66p9bk test		vpc-s1e2bu0d test2	subnet-mc4zf132 aa

Modifying a Network Probe

1. Log in to [VPC console](#).
2. Select **Diagnostic Tools** -> **Network Probe** in the left sidebar to enter the management page.
3. In the list, locate the network probe to modify and click **Edit** in the **Operation** column.



ID/Name	Monitoring	Virtual Private Cloud	Subnet	Source IP	Next hop	Destination IP to probe	Notes	Operation
netd-ap66p9bk test		vpc-s1e2bu0d test2	subnet-mc4zfl32 aa	192.168.2.11 192.168.2.2	nat-mqinoi8 test		-	Edit Delete

4. In the **Edit Network Probe** pop-up window, make required changes and click **Submit** to save the changes.

Note:

This example has no next hop specified.

If no next hop is specified, the name, probe destination IP, and notes of the network probe can be modified.

If a next hop is specified, the name, probe destination IP, source next hop, and notes of the network probe can be modified.

Edit Network Probe

Name

test

Virtual Private Cloud

test2 (vpc-s1e2bu0d | 192.168.0.0/16)

Subnet

aa (subnet-mc4zfl32 | 192.168.2.0/24) Guangzhou Zone 1

Destination IP to probe

9

Verify

Optional

Verify

Next hop

NAT Gateway

nat-rnqinoi8 (test)

Statistical Method

Average

Notes

Submit





Cancel

Deleting a Network Probe

1. Log in to [VPC console](#).
2. Select **Diagnostic Tools** -> **Network Probe** in the left sidebar to enter the management page.
3. In the list, locate the network probe to delete and click **Delete** in the operation column.
4. Click **Delete** in the pop-up window to confirm the deletion.

Note:

Deleting a network probe also deletes all associated alarming policies and configured routes. Check whether your business will be affected before continuing.

ID/Name	Monitoring	Virtual Private Cloud	Subnet	Source IP	Next hop	Destination IP to probe	Notes	Operation
netd-ap66p9bk test 		vpc-s1e2bu0d test2	subnet-mc4zfl32 aa	192.168.2.11 192.168.2.2	nat-mqinol8 test		- 	Edit Delete

Confirm to delete the object

BLANK, and the associated alarm policies and the routing configuration of network probe will also be deleted.

[Delete](#) [Cancel](#)

Configuring an Alarm Policy

You can configure an alarm policy for the network probe service, so that you can promptly detect any route exception to help switch routes quickly and ensure business availability.

1. Log in to the CM console and go to the [Alarm Policy](#) page.
2. Click **Create**. In the **Create Alarm Policy** pop-up window, enter the policy name, select **Network Probe** for the policy type, configure the alarm object, alarm trigger condition and alarm policy, and click **Complete**.

Instance Port Verification

Last updated : 2024-10-22 16:20:53

The instance port verification feature can help you detect the port accessibility of a security group associated with CVM instances, locate faults, and improve the user experience.

This feature supports the accessibility detection of common ports and custom ports. See below for the common ports.

Rule	Port	Description
Inbound rules	ICMP protocol	Used to pass control messages such as the ping command. ICMP is a control protocol, and no ports are involved.
	TCP:20	Used to allow uploads and downloads over FTP.
	TCP:21	
	TCP:22	Used to allow Linux SSH login.
	TCP:3389	Used to allow Windows remote login.
	TCP:443	Used to provide website HTTPS service.
	TCP:80	Used to provide website HTTP service.
Outbound rules	ALL	Used to allow all outbound traffic for access to external networks.

Operation Guide

1. Log in to the [VPC console](#).
2. Click **Diagnostic Tools > Port Verification** in the left sidebar to access the management page.
3. Select a region at the top of the page, locate the instance you want to verify in the list, and click **Quick Check**.

Port Verification Guangzhou

ID/Name	Connectivity Diagnosis	IP address
ins-	Quick Check	

4. You can see the port detection details in the pop-up window. Perform the following operations as needed.

Uncheck the port that you do not want to detect.

Enter custom ports to detect and click **Save**.

Protocol: select TCP or UDP.

Port: enter one port number to detect, which cannot be the same as a common port.

Direction: select **Inbound** or **Outbound**.

IP: enter the source IP for the inbound direction and destination IP for the outbound direction. Enter **ALL** for all source and destination IP addresses.

Up to 15 custom ports can be detected.

If you need to detect the outbound traffic towards IP 10.0.1.12 using TCP protocol through port 30, enter the following information in the **Custom port detection** area.

Port Detection

<input checked="" type="checkbox"/>	Protocol	Port	Direction	Policy	Effects
<input checked="" type="checkbox"/>	ICMP	-	Inbound	Open	None
<input checked="" type="checkbox"/>	TCP	20	Inbound	Open	None
<input checked="" type="checkbox"/>	TCP	21	Inbound	Open	None
<input checked="" type="checkbox"/>	TCP	22	Inbound	Open	None
<input checked="" type="checkbox"/>	TCP	3389	Inbound	Open	None
<input checked="" type="checkbox"/>	TCP	443	Inbound	Open	None
<input checked="" type="checkbox"/>	TCP	80	Inbound	Open	None
<input checked="" type="checkbox"/>	ALL	ALL	Outbound	Open	None

Custom port detection

Protocol	Port	Direction	IP ⓘ	Policy	Operation
<div>TCP</div>	<div>Example: 80</div>	<div>Inbound</div>	<div>Enter the IP</div>		<div>Save</div>

15 more ports can be added

Detect

5. After completing the configuration, click **Detect**. The result will be displayed in the **Policy** column.

Custom port detection					
Protocol	Port	Direction	IP ⓘ	Policy	Operation
TCP	30	Outbound	10.0.1.12	Open	Delete

Assumes that you need to open an Not opened port, for example TCP:22,

<input checked="" type="checkbox"/> TCP	22	Inbound	Not opened	Unable to use SSH
---	----	---------	------------	-------------------

Then you can add an inbound rule for the security group associated with the instance in the [Security Group console](#) to open port TCP:22. You can select all for Source to allow all IPs, or enter a specific IP (IP range).

Add inbound rule

Type	Source i	Protocol Port i	Policy	Notes
Login Linux CVMs(22) ▼	all	TCP:22	Allow ▼	TCP port 22 open for Linux
<div>+New Line</div>				
<div>Complete</div>			<div>Cancel</div>	

Relevant Information

For information on security groups, see [Security Group Overview](#) and [Adding a Security Group Rule](#).

For more information on common ports, see [Common Server Ports](#).

Flow Logs

Last updated : 2024-10-22 16:25:32

Flow Logs (FL) provide a real-time, full-flow, and non-intrusive traffic capture service so you can store and analyze network traffic in real time, helping you to conduct troubleshooting, architecture optimization, security testing, and compliance auditing.

Common Operations

[Creating flow logs](#)

[Creating logsets and log topics](#)

[Deleting flow logs](#)

[Viewing flow log entries](#)

Traffic Mirroring

Overview

Last updated : 2024-10-22 16:25:49

Traffic mirror provides a traffic collection service that filters and copies desired traffic from the specified network interface to CVM instances in the same VPC. This feature is applicable to use cases including security audit, risk monitoring, troubleshooting and business analysis.

Note:

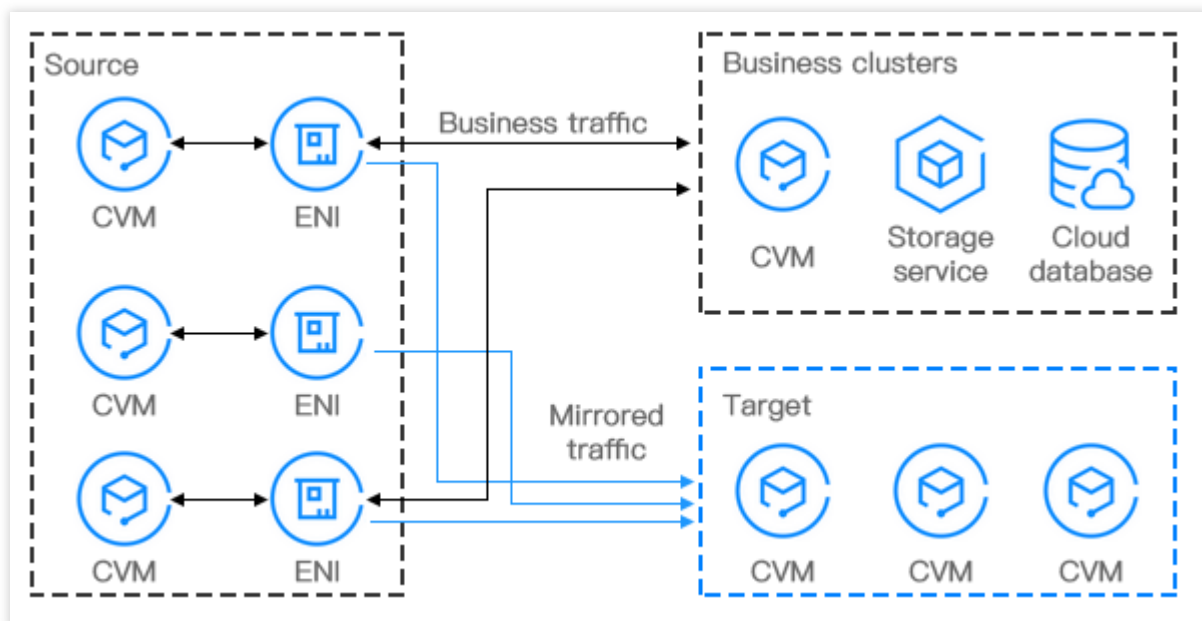
However, traffic mirror consumes CVM resources such as CPU, memory and bandwidth pro rata. For example, if you mirror a network interface that has 1 Gbps of inbound traffic and 1 Gbps of outbound traffic. In this case, the instance needs to handle 1 Gbps of inbound traffic and 3 Gbps of outbound traffic (1 Gbps for the outbound traffic, 1 Gbps for the mirrored inbound traffic and 1 Gbps for the mirrored outbound traffic).

Procedure

The following are key components of a traffic mirror, together with its workflow.

Source: the specified ENI in the VPC that applies the filter rules such as network, collection range, collection type and traffic filtering.

Target: the receiving IPs that get the collected traffic.



Use Cases

Security auditing

A running system may occur unhealthy network traffic or generate an error message due to software exception, hardware fault, computer virus or improper use. To locate causes of these issues, you can use traffic mirror to analyze the network messages.

Intrusion checking

To ensure the confidentiality, integrity and availability of network system resources, you can use traffic mirror to copy traffic to CVM clusters for real-time analysis.

Business analysis

Use traffic mirror to clearly and visually present the business traffic mode.

Use Limits

Last updated : 2024-10-22 16:26:06

Assess the following limits before using a traffic mirror, so that your businesses will not be affected.

The traffic mirror feature is currently in beta test. To try it out, [submit a ticket](#) for application. Save the link to the Traffic Mirror console for later logins; otherwise, you may need to apply again.

Using the traffic mirror feature will consume the CPU, memory, bandwidth, and other resources of the server.

Mirrored traffic will be included in the instance bandwidth, and the impact on system resources depends on your traffic volume and type. For example, if a network interface has 1 Gbps inbound traffic and 1 Gbps outbound traffic and uses the traffic mirror feature, its application system will need to handle 1 Gbps inbound traffic and 3 Gbps outbound traffic (including 1 Gbps outbound traffic, 1 Gbps mirrored inbound traffic, and 1 Gbps mirrored outbound traffic).

Flow logs cannot be used to capture traffic mirror data.

Security group limits:

Collection source: Mirrored traffic is not subject to security group policies.

Receiver: It is subject to security group policies.

Traffic mirror cannot be used for the following data services:

ARP

DHCP

Instance metadata service

NTP

Windows activation

The collection source and the receiver of a traffic mirror support the following models:

Standard S1, Standard S2, Standard S3, Memory Optimized M1, M2, M3 and M6, High IO I1, I2, and I3, Compute C2 and C3, Compute Enhanced CN3, and Big Data D1.

CVM ENIs are subject to the following limits:

When a traffic mirror is set, the upper ENI bandwidth limit of the target CVM instance must be at least 1/9 of the total ENI bandwidth of all CVM instances in the collection scope.

For example, if there are six S3.6XLARGE48 instances in the collection scope of a traffic mirror, and the total ENI bandwidth is $3 \text{ Gbps} * 6 = 18 \text{ Gbps}$, then the inbound bandwidth at the receiver must be at least 2 Gbps ($18/9 = 2$), that is, at least two S3.MEDIUM8 instances or one S3.4XLARGE32 instance.

To avoid the situation where the mirrored traffic exceeds the capacity of the receiving ENI, increase the number of receivers and CVM instance specifications to cater to the business traffic volume. For more information on CVM instance specifications, see [Instance Types](#).

Creating Traffic Mirror

Last updated : 2024-10-22 16:26:22

A traffic mirror provides a traffic collection service that enables you to filter the traffic from the specified ENI by using quintuple and other rules. Then you can copy the filtered traffic to CVM instances in the same VPC. This feature is applicable to use cases including security audit, risk monitoring, troubleshooting, and business analysis. This document describes how to create a traffic mirror.

Note:

The traffic mirror feature is currently in beta test. To try it out, [submit a ticket](#) for application. Save the link to the Traffic Mirror console for later logins; otherwise, you may need to apply again.

Prerequisites

Make sure that the source IP and target ENI are in the same VPC and that the source IP has a route table pointing to the target ENI.

Directions

Step 1. Create a traffic mirror source

1. Log in to the [VPC console](#).
2. Click **Diagnostic Tools** > **Traffic Mirror** on the left sidebar and select the target region.
3. Click **+New**.

Note:

Up to five traffic mirrors can be created in a VPC.

4. In the pop-up window, configure as follows:
Enter the traffic mirror name (up to 60 characters).

Choose **Network**.

Select **ENI** for **Collection Scope**. That is, all traffic in the VPC will be collected, excluding the traffic of the ENI that is bound to the receiving IPs. If you select this option, you need to select the specific ENI.

Collection Range **ENI**

Please select an ENI

Enter an ENI ID/Name

☒ eni-111

Selected ENI

eni-111

Select **Collection type**: Select the traffic direction as needed. There are three options: **All traffic**, **Traffic out**, and **Traffic in**.

Select **Traffic filtering**: Select a method to filter out unnecessary traffic and keep the mirror small and lightweight.

N/A: All traffic configured will be collected.

Quintuple: The traffic that meets quintuple conditions will be collected. After selecting this option, specify **Protocol**, **Source IP range**, **Destination IP range**, **Source port**, and **Destination port**. You can click **Add** to create another filter. Only the traffic that meets all of the filters will be collected.

Traffic filtering **Quintuple**

Condition

Protocol	Source IP range ⁱ	Destination IP range ⁱ	Source Port	Destination p
ALL				

[Add](#) [Delete](#)

The next hop is the NAT gateway: Collect traffic whose next hop address is the NAT gateway. After selecting this option, select the specific NAT gateway next to **Condition**.

5. After completing the configuration, click **Next**.

Step 2. Create a traffic mirror target

1. On the **Create Traffic Mirror Target** page, configure the following items:

Target type: Select the target ENI to receive the forwarded traffic.

Note:

At least one target ENI needs to be selected.

Traffic to the target ENI from inside the VPC will not be collected.

Balance method:

Evenly distribute traffic: All traffic is distributed among all target ENIs evenly.

HASH by ENI: Traffic from an ENI is always forwarded to a fixed target ENI.

Target type

ENI

Please select an ENI

Enter an ENI ID/Name

eni-222

Selected ENI

eni-222

Balance method

☒ Evenly distribute traffic ⓘ

☐ HASH by ENI ⓘ

[Advanced Options >](#)

OK

Previous

2. Click **OK**.

Result Validation

Note:

This document takes creating a traffic mirror that collects the outbound traffic of the 10.0.0.14 ENI accessing the www.qq.com website as an example.

1. Return to the **Traffic Mirror** page. If the created traffic mirror is displayed in the list with **Collect Traffic** enabled, it has been created successfully.

Name/ID	Collection Range	Collection Type	Network	Creation Time	Collect Traffic	Operation
imgf-d imager	ENI	Traffic out	vpc-k5 Default	2020-11-02 15:05:18	<input checked="" type="checkbox"/>	Edit Tags Delete

2. Perform the following steps to verify whether the collected traffic is mirrored to the receiving IP.

2.1 Generate the ENI traffic. For example, you can log in to the source CVM and run the "ping **public IP**" command.

Source data:

```
[root@VM-0-14-centos ~]# ping www.qq.com
PING https.qq.com (58.250.137.36) 56(84) bytes of data.
64 bytes from 58.250.137.36 (58.250.137.36): icmp_seq=1 ttl=56 time=4.55 ms
64 bytes from 58.250.137.36 (58.250.137.36): icmp_seq=2 ttl=56 time=4.61 ms
64 bytes from 58.250.137.36 (58.250.137.36): icmp_seq=3 ttl=56 time=4.61 ms
64 bytes from 58.250.137.36 (58.250.137.36): icmp_seq=4 ttl=56 time=4.62 ms
64 bytes from 58.250.137.36 (58.250.137.36): icmp_seq=5 ttl=56 time=4.58 ms
64 bytes from 58.250.137.36 (58.250.137.36): icmp_seq=6 ttl=56 time=4.57 ms
64 bytes from 58.250.137.36 (58.250.137.36): icmp_seq=7 ttl=56 time=4.57 ms
64 bytes from 58.250.137.36 (58.250.137.36): icmp_seq=8 ttl=56 time=4.59 ms
64 bytes from 58.250.137.36 (58.250.137.36): icmp_seq=9 ttl=56 time=4.58 ms
64 bytes from 58.250.137.36 (58.250.137.36): icmp_seq=10 ttl=56 time=4.60 ms
64 bytes from 58.250.137.36 (58.250.137.36): icmp_seq=11 ttl=56 time=4.57 ms
64 bytes from 58.250.137.36 (58.250.137.36): icmp_seq=12 ttl=56 time=4.62 ms
^C
--- https.qq.com ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 27ms
rtt min/avg/max/mdev = 4.548/4.588/4.619/0.065 ms
```

2.2 Log in to the destination CVM and run the following command to capture data and save it as a `.cap` or `.pcap` file. This document uses the `.pcap` file as an example.

```
tcpdump -i eth0 -w capture-2020-10-27.pcap # Enter the actual filename.
```

Destination packets:

```
[root@VM-0-11-centos ~]# tcpdump -i eth0 -w capture-2020-10-27.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C721 packets captured
735 packets received by filter
0 packets dropped by kernel
[root@VM-0-11-centos ~]# ls
capture-2020-10-27.pcap
```

2.3 Use a terminal simulator (such as SecureCRT) to log in to the destination CVM and export the file saved in [Step ii](#).

```
sz -bye capture-2020-10-27.pcap
```

2.4 Use a packet parser (such as Wireshark) to get the data from the downloaded `capture-2020-10-27.pcap` file. In this sample, 12 mirrored packets of the source CVM instance are obtained from the destination CVM instance.

Packet verification:

capture-2020-10-27.pcap

Apply a display filter ... <3%>

No.	Time	Source	Destination	Protocol	Length	Info
369	26.523196	10.0.0.14	58.250.137.36	ICMP	98	Echo (ping) request id=0x251b, seq=1/256, ttl=64 (no response)
375	27.524318	10.0.0.14	58.250.137.36	ICMP	98	Echo (ping) request id=0x251b, seq=2/512, ttl=64 (no response)
387	28.525991	10.0.0.14	58.250.137.36	ICMP	98	Echo (ping) request id=0x251b, seq=3/768, ttl=64 (no response)
409	29.527690	10.0.0.14	58.250.137.36	ICMP	98	Echo (ping) request id=0x251b, seq=4/1024, ttl=64 (no response)
426	30.529380	10.0.0.14	58.250.137.36	ICMP	98	Echo (ping) request id=0x251b, seq=5/1280, ttl=64 (no response)
443	31.531020	10.0.0.14	58.250.137.36	ICMP	98	Echo (ping) request id=0x251b, seq=6/1536, ttl=64 (no response)
465	32.532644	10.0.0.14	58.250.137.36	ICMP	98	Echo (ping) request id=0x251b, seq=7/1792, ttl=64 (no response)
482	33.534324	10.0.0.14	58.250.137.36	ICMP	98	Echo (ping) request id=0x251b, seq=8/2048, ttl=64 (no response)
487	34.535641	10.0.0.14	58.250.137.36	ICMP	98	Echo (ping) request id=0x251b, seq=9/2304, ttl=64 (no response)
503	35.536630	10.0.0.14	58.250.137.36	ICMP	98	Echo (ping) request id=0x251b, seq=10/2560, ttl=64 (no response)
518	36.537354	10.0.0.14	58.250.137.36	ICMP	98	Echo (ping) request id=0x251b, seq=11/2816, ttl=64 (no response)
541	37.538718	10.0.0.14	58.250.137.36	ICMP	98	Echo (ping) request id=0x251b, seq=12/3072, ttl=64 (no response)

Fragment offset: 0
Time to live: 64
Protocol: ICMP (1)
Header checksum: 0xc788 [validation disabled]
[Header checksum status: Unverified]
Source: 10.0.0.14
Destination: 58.250.137.36

0000 52 54 00 d8 16 3e fe ee 7f 99 99 19 08 00 45 00 RT...>... E.
0010 00 54 a4 f4 40 00 01 c7 88 0a 00 00 0e 3a fa .T...@... :.
0020 89 24 08 00 be 7b 25 1b 00 01 8a 28 98 5f 00 00 .\$....{%. ... (._..
0030 00 00 25 0d 0e 00 00 00 00 10 11 12 13 14 15 ...%.....
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 !"#%\$
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*+,-./012345
0060 36 37 67

3. If an abnormal packet is obtained or packets cannot be obtained, [submit a ticket](#) for assistance.

Subsequent Operations

[Enabling and Disabling a Traffic Mirror](#)

[Modifying a Traffic Mirror](#)

[Adding Tags](#)

[Deleting a Traffic Mirror](#)

Managing Traffic Mirror


Last updated : 2024-10-22 16:26:42

After a traffic mirror is created, you can enable, disable, modify or delete it or add tags on the console.

Enabling and Disabling a Traffic Mirror

A new traffic mirror task is enabled by default. To disable it and then enable it again, follow the steps below.

1. Log in to the [VPC console](#).
2. Click **Diagnostic Tools > Traffic Mirror** on the left sidebar and select the target region.
3. Locate the traffic mirror you want to manage, disable or enable it under the **Collect traffic** column.

<div>+ New</div>						
Name/ID	Collection Range	Collection Type	Network	Creation Time	Collect Traffic	Operation
imgf- [redacted]	ENI	All traffic	vpc- [redacted]	2022-02-11 16:03:47		Edit Tags Delete

Modifying a Traffic Mirror

To modify an existing traffic mirror, follow the steps below:

1. Log in to the [VPC console](#).
2. Click **Diagnostic Tools > Traffic Mirror** on the left sidebar and select the target region.
3. Select the Name/ID of the traffic mirror to be modified.
4. Modify the desired items.

Edit traffic collection configurations

- 4.1.1 Click **Edit** on the top-right corner of the Traffic Collection section.
- 4.1.2 In the pop-up window, modify **Collection ENI**, **Collection type**, **Traffic filtering** and other configurations as needed, and then click **OK**.

Edit traffic receiving configurations

- 4.1.1 Click **Edit** on the top-right corner of the Traffic Receiving section.
- 4.1.2 In the pop-up window, modify **Target ENI** and **Balance mode**, and then click **OK**.

Traffic Collection Configurations		Traffic Receiving Configurations			
Target ENI	<table border="1"><thead><tr><th>ID/Name</th></tr></thead><tbody><tr><td>eni-111</td></tr></tbody></table>	ID/Name	eni-111	Target type	ENI
ID/Name					
eni-111					
Collection Type	All traffic	ENI	<table border="1"><thead><tr><th>ID/Name</th></tr></thead><tbody><tr><td>eni-222</td></tr></tbody></table>	ID/Name	eni-222
ID/Name					
eni-222					
Traffic filtering	N/A	Balance method	Evenly distribute traffic ⓘ		

Adding Tags

Tags are used to identify and organize Tencent Cloud resources. Each tag contains a tag key and a tag value. Adding a tag to the traffic mirror makes it easy to filter and manage traffic mirror resources.

1. Log in to the [VPC console](#).
2. Click **Diagnostic Tools** > **Traffic Mirror** on the left sidebar and select the target region.
3. Locate the traffic mirror to which you want to add tags, and click **Edit tags** under the **Operation** column.
4. In the pop-up dialog box, configure as follows:
 - 4.1 For **Tag key**, enter the key name or select from the drop-down list.
 - 4.2 For **Tag value**, enter the key value.

Note:

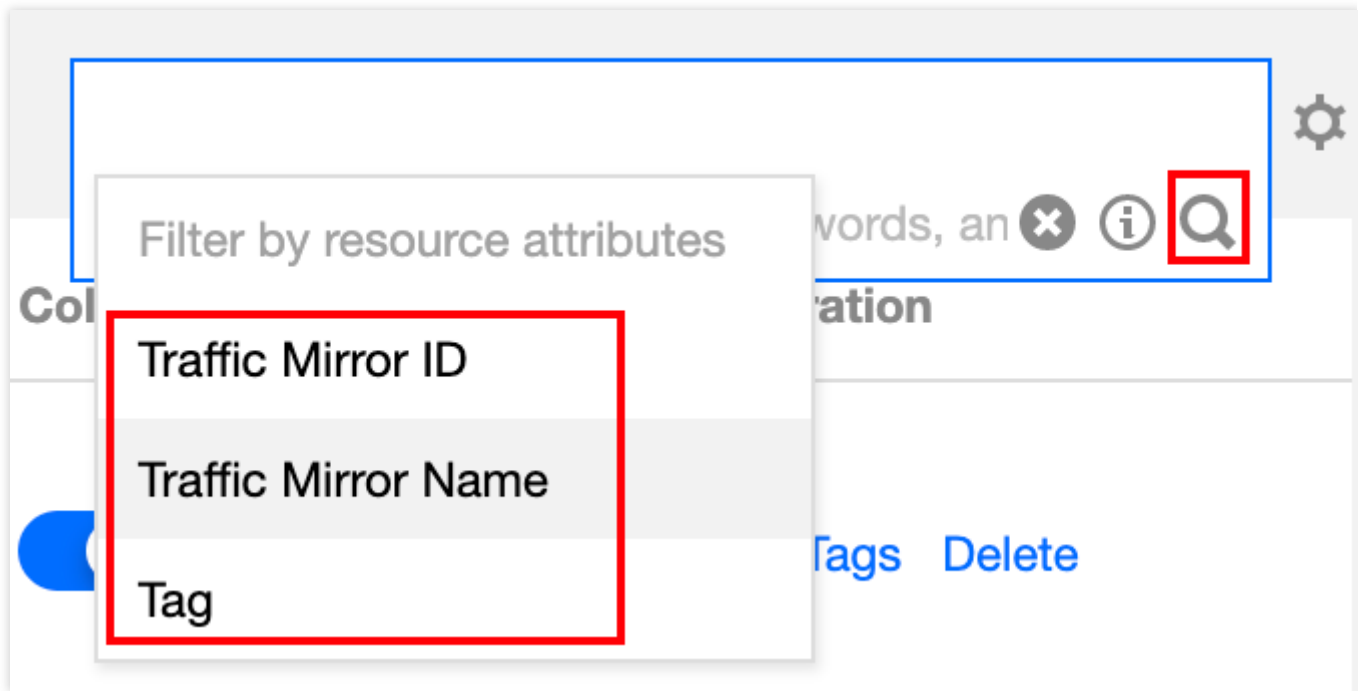
- A tag key may have none or many tag values.
- 4.3 (Optional) Click **Add** and configure **Tag key** and **Tag value** to add a tag.
 - 4.4 After completing the configuration, click **OK**.

Locating a Traffic Mirror

1. Click



in the top right of the **Traffic mirroring** page and select a filter. Three filters as shown in the following figure are available.



2. Enter a keyword in the edit box and click



Note:

Separate keywords with vertical bars (|).

Deleting a Traffic Mirror

1. Log in to the [VPC console](#).
2. Click **Diagnostic Tools** > **Traffic Mirror** on the left sidebar and select the target region.
3. Locate the traffic mirror to be deleted, click **Delete** under the **Operation** column, and confirm the deletion.

Snapshot Policy

Overview

Last updated : 2024-10-22 16:27:02

A snapshot allows you to back up the associated object data according to the configured backup policy. Currently, it can be associated with a security group, so that you can back up the outbound and inbound rules of the associated security group. This feature is an auxiliary feature which does not affect the operations on security groups.

Note:

The snapshot feature is currently in beta test. To try it out, [submit a ticket](#) for application.

Use Cases

If you need to frequently update your security group rules, we recommend you configure a snapshot policy for the security group and promptly back up the security group rules. When the newly modified rules are abnormal, you can use the snapshot rollback feature to roll back to the original rules, thus ensuring the business availability.

Use Limits

Resource	Quota
Maximum number of snapshot policies that can be created by a user	5
Number of time points that can be set in each scheduled snapshot policy	5
Number of snapshot policies that can be associated with an object (security group)	1
Number of objects (security groups) that can be associated with a snapshot policy	50
Maximum retention period of the scheduled snapshot policy	365 days
Backup change frequency	Five times per ten seconds

Creating Snapshot Policy

Last updated : 2024-10-22 16:39:45

When you need to back up security group rules to meet subsequent business needs or roll back to the original rules due to new rule exceptions, you can configure a snapshot policy.

Note:

Authorize the COS service: As snapshot records are stored in a COS bucket, you need to perform read and write operations on COS. If you have not authorized the COS service when creating the snapshot policy, the system will automatically pop up a window for you to perform authorization as prompted. After performing the authorization, you can refresh the page to go to the snapshot policy page. No more authorization is required after that.

Directions

1. Log in to the [VPC console](#) and choose **Diagnostic Tools > Snapshot policy** in the left sidebar.
2. Click **Create**.
3. In the **Create snapshot policy** pop-up window, configure the parameters.

Parameter	Description
Name	Customize the snapshot policy name, which can contain digits, letters, and special symbols.
Backup Policy	Operation-triggered backup and scheduled backup are supported: Operation-triggered backup: A backup is triggered each time the security group rule is "operated". Note : Currently, you can perform up to five operations per ten seconds. More frequent operations will not be recorded. Scheduled backup: Backups are performed at fixed time points.
Backup start time	This parameter is displayed only when you select Scheduled Backup . The date ranges from Monday to Sunday, and the time can be accurate to the second. Up to five backup times can be added, and at least one is retained. Note : The backup operation is affected by the data volume. When the data volume is large, there may be some deviation between the selected time point and the actual time point.
Snapshot Retention	You can customize the retention period of backup records, after which the records will be deleted automatically. The maximum value is 365 days.
Creating COS	Yes: Create a COS bucket.

Bucket	No: Use an existing COS bucket.
COS Bucket	<p>If you choose to create a COS bucket, select the region and enter the COS bucket name, which cannot be changed once set. The name can contain lowercase letters, digits, and hyphens, and the access domain name must contain less than 60 characters. If you select an existing COS bucket, select the region and the bucket name, which cannot be changed once selected.</p> <p>Note :</p> <p>The backup information is stored in a COS bucket. After the bucket is deleted, the snapshot information cannot be queried or restored.</p>
COS bucket name	A COS bucket name is in the format of Custom name - Developer app ID. A COS bucket name can contain up to 60 characters, including letters, digits, and hyphens (-). A COS bucket name cannot be changed once set.

4. Click **OK**.

Related Operations

[Associating Security Group](#)

Associating, Disassociating, and Querying Security Group

Last updated : 2024-10-22 16:40:01

After creating a snapshot policy, you can associate it with security groups. Security groups added to the snapshot list will be backed up according to the policy and can be disassociated when snapshot backup is no longer needed. This document describes how to associate and disassociate security groups with/from a snapshot policy and how to view the associated security groups.

Prerequisites

You have created a snapshot policy.

You have prepared security groups to be associated.

Associating Security Group

1. Log in to the [VPC console](#) and select **Diagnostic Tools > Snapshot Policy** on the left sidebar.
2. On the **Snapshot Policy** page, click the snapshot policy ID to enter the details page.
3. Click **Associate Security Group**.
4. On the **Associate Security Group** page, select the **Region** and click the arrow icon on the right of the security groups to be associated in the **Select** list. The selected security groups are displayed in the **Selected** list on the right. Click **OK**.

Note:

A snapshot policy is not specific to a region and can be associated with security group instances in all regions.

However, only security groups in the same region can be associated with at a time. To associate a snapshot policy with security groups in different regions, perform multiple association operations.

A security group can be associated with only one snapshot policy.

Disassociating Security Group

1. Log in to the [VPC console](#) and select **Diagnostic Tools > Snapshot Policy** on the left sidebar.
2. On the **Snapshot Policy** page, click the snapshot policy ID to enter the details page.
3. Click **Disassociate** on the right of the security group to be disassociated.

4. In the **Disassociate Security Group** pop-up window, confirm the information and click **OK**. The security group rules will no longer be backed up, but the existing backup records will not be deleted.
5. (Optional) To disassociate multiple security groups at a time, select them, click **Batch Disassociate** at the top, and click **OK** in the pop-up window.

Note:

Only security groups in the same region can be disassociated at a time.

Querying Security Group

To query the security groups associated with a snapshot policy, follow the instructions below.

1. Log in to the [VPC console](#) and select **Diagnostic Tools > Snapshot Policy** on the left sidebar.
2. On the **Snapshot Policy** page, click the snapshot policy ID to enter the details page.
3. In the **Associated Security Groups** section, you can view all the security groups associated with the snapshot policy.
4. Click the filter icon next to the region to filter security groups by region. Click the settings icon in the top-right corner to customize the list fields.
5. Click the **Security Group ID** to enter the security group details page.

Enabling and Disabling Snapshot Policy

Last updated : 2024-10-22 16:40:18

A successfully created snapshot policy is enabled by default. This document describes how to disable and enable it again when needed. Disabling it will stop generating snapshot backups of all its associated security groups without deleting the original backup information.

Disabling Policy

After the policy is disabled, no more backups will be performed but the original backup information will not be deleted.

1. Log in to the [VPC console](#) and select **Diagnostic Tools > Snapshot Policy** on the left sidebar.
2. On the **Snapshot Policy** page, click the snapshot policy ID to enter the details page. The blue toggle button in the figure indicates that the policy is enabled.
3. Click the button, confirm the impact in the **Disable Snapshot Policy** pop-up window, and click **OK**.

The disabled policy is as shown below:

Enabling Policy

After the policy is disabled, you can enable it again as instructed below. Then the associated security group rules will continue to be backed up according to the previously configured policy.

1. Click the **Enable Policy** toggle.
2. In the **Enable Snapshot Policy** pop-up window, click **OK**.

Modifying Snapshot Policy

Last updated : 2024-10-22 16:41:53

You can modify the name, retention period, and backup time of a snapshot policy as instructed below.

Directions

1. Log in to the [VPC console](#) and select **Diagnostic Tools > Snapshot Policy** on the left sidebar.
2. On the **Snapshot Policy** page, click **Modify Policy** on the right of the target policy.
3. In the **Modify Snapshot Policy** pop-up window, make changes as needed.

For **Operation-Triggered Backup**, you can modify the policy name and snapshot retention period.

For **Scheduled Backup**, you can modify the policy name, backup time, and snapshot retention period.

4. Click **OK**.

Querying Snapshot Policy

Last updated : 2024-10-22 16:42:07

The **Snapshot Policy** page displays the details of all created snapshot policies, including policy name, COS bucket, backup policy, retention period, creation time, policy status, and related executable operations.

Directions

1. Log in to the [VPC console](#) and select **Diagnostic Tools > Snapshot Policy** on the left sidebar.
2. On the **Snapshot Policy** page, you can view the list of all created snapshot policies.
3. Click the policy **ID** to view its basic information and associated security group.
4. Click the COS bucket name to view the bucket details.
5. Click the settings icon in the top-right corner to customize the list fields.
6. Click the refresh icon in the top-right corner to refresh the information displayed on the page.

Deleting Snapshot Policy

Last updated : 2024-10-22 16:42:26

This document describes how to delete a snapshot policy if you no longer need to generate snapshot backups of security group rules but need to delete the backup records of all security group rules associated with the snapshot policy.

Directions

1. Log in to the [VPC console](#) and select **Diagnostic Tools > Snapshot Policy** on the left sidebar.
2. On the **Snapshot Policy** page, click **Delete** on the right of the target snapshot policy.
3. In the confirmation pop-up window, confirm the impact and click **OK**.

Note:

Note that after the deletion, all security group rules associated with the snapshot policy will no longer be backed up, and the existing backup records will be deleted.

Alarming and Monitoring

Last updated : 2024-10-22 16:42:42

By configuring alarm policies, you can monitor the status of resources on a VPC, such as NAT gateway, VPN gateway, direct connect gateway, EIP, etc., so as to discover the abnormal running of cloud resources in time, locate and solve problems ASAP.

Configuring an Alarm Policy

1. Log in to the [Cloud Monitor console](#).
2. Select **Alarm Configuration** > **Alarm Policy** in the left sidebar to enter the alarm policy configuration page.
3. Click **Create**, enter a policy name, select a VPC cloud resource to be configured for policy type, such as **VPC** > **EIP**, and then configure alarm rules and alarm notifications.
4. Click **Complete**. You can see the set alarm policy in the alarm policy list.

Note:

To delete an alarm policy, you need to first unbind all resources from it.

5. When an alarm is triggered, you will receive the alarm notification through the selected alarm channel (SMS / email/ Message Center, etc.).

Alarm policy configurations for different cloud resources are detailed below:

Direct Connect: [Configuring Alarm Policies](#)

NAT Gateway: [Setting Alarms](#)

VPN Connection: [Setting Alarms](#)

Viewing Monitoring Information

You can view the monitoring information of the corresponding cloud resources in the VPC console to help you troubleshoot the network failures. See:

Direct Connect: [Viewing Monitoring Data](#)

CCN: [View Monitoring Information](#)

NAT Gateway: [Viewing Monitoring Information](#)

Peering Connection: [Viewing Monitoring Data of Network Traffic Over a Cross-region Peering Connection](#)

VPN Connection: [Viewing Monitoring Data](#)