

# 私有网络 操作指南



腾讯云

---

**【 版权声明 】**

©2013–2024 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分內容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

**【 商标声明 】**

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

**【 服务声明 】**

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。

您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

**【 联系我们 】**

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

## 文档目录

### 操作指南

#### 网络拓扑

#### 网络性能大盘

#### 私有网络

##### 概述

##### 限制说明

##### 创建私有网络

##### 查看私有网络

##### 编辑 IPv4 CIDR

##### 编辑 IPv6 CIDR

##### 修改私有网络 DNS 信息

##### 修改私有网络名称和标签

##### 关联或解关联云联网

#### 基础网络互通

##### 概述

##### 管理基础网络互通

##### 开启或关闭组播功能

##### 删除私有网络

#### 子网

##### 创建子网

##### 查看子网

##### 获取与释放 IPv6 CIDR

##### 更换子网路由表

##### 管理 ACL 规则

##### 开启或关闭广播

##### 删除子网

#### 路由表

##### 概述

##### 限制说明

##### 创建自定义路由表

##### 关联与解关联子网

##### 管理路由策略

##### 删除路由表

#### IP 与 网卡

##### 弹性公网 IP

##### 弹性公网 IPv6

##### 高可用虚拟 IP

###### 概述

###### 限制说明

###### 创建高可用虚拟 IP

###### 绑定或解绑 EIP

###### 查询高可用虚拟 IP

###### 释放高可用虚拟 IP

##### 弹性网卡

#### 共享带宽包

#### 共享流量包

#### 网络连接

##### NAT 网关

##### VPN 连接

##### 专线接入

##### 云联网

##### 私有连接

## 安全管理

### 安全组

安全组概述

创建安全组

添加安全组规则

关联实例至安全组

安全组修改项目信息

管理安全组

查看安全组

移出安全组

克隆安全组

删除安全组

调整安全组优先级

管理安全组规则

查看安全组规则

修改安全组规则

删除安全组规则

导入安全组规则

导出安全组规则

排序安全组规则

快照回滚

安全组应用案例

服务器常用端口

### 网络 ACL

规则概述

限制说明

管理网络 ACL

### 参数模板

概述

限制说明

管理参数模板

配置案例

### 访问管理

访问管理概述

可授权的资源类型

VPC 访问管理策略示例

VPC API 操作支持的资源级权限

## 诊断工具

### 网络探测

#### 实例端口验通

#### 网关流控

#### 网络流日志

### 流量镜像

流量镜像概述

使用限制

创建流量镜像

管理流量镜像

### 快照策略

概述

创建快照策略

关联、解绑、查询安全组

启用和关闭快照策略

修改快照策略

查询快照策略

删除快照策略

告警与监控

API 2.0 切换 API 3.0 指引

## 操作指南

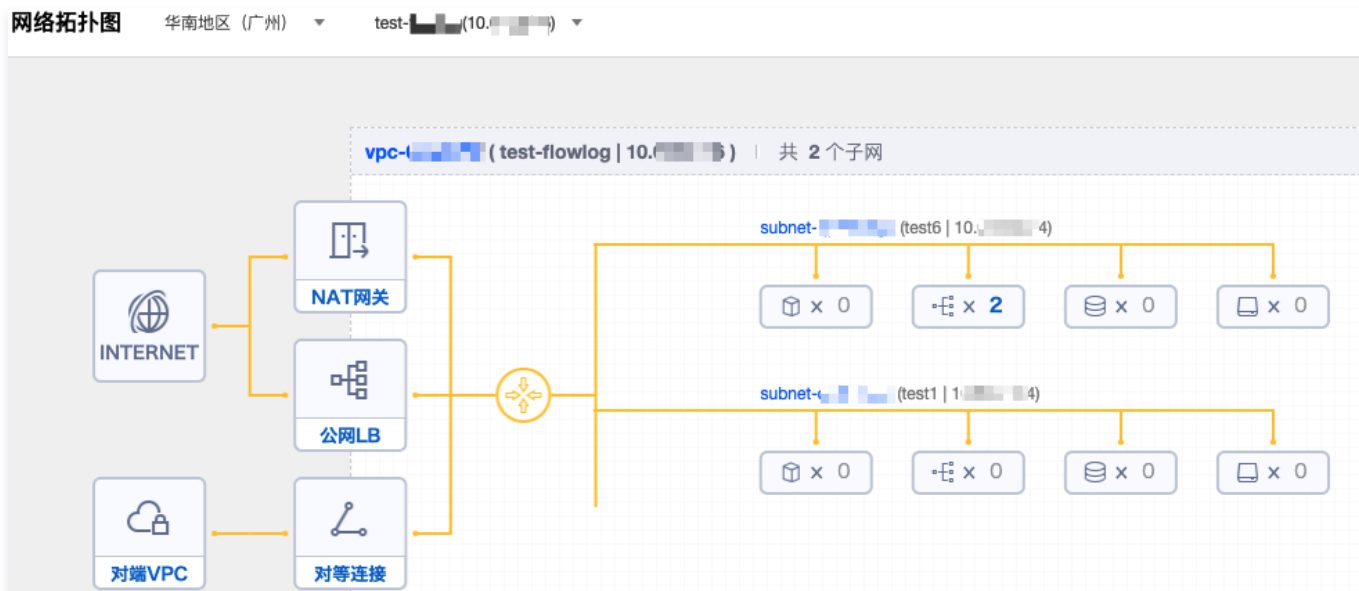
### 网络拓扑

最近更新时间：2024-03-20 17:08:41

网络拓扑用于查看私有网络下包含的所有资源，以便您实时了解私有网络的资源部署及网络连接情况。

### 操作步骤

1. 登录 [私有网络控制台](#)。
2. 单击左侧导航中的**网络拓扑**，进入网络拓扑图的展示界面。
3. 选择地域、私有网络，可查看该私有网络中包含的云资源（如云服务器、负载均衡、云数据库 MySQL、云缓存 Memcached），及网络拓扑关系。  
例如，如下图所示，该 VPC 包含两个子网，其中子网 test6 中包含2个负载均衡实例，该 VPC 通过 NAT 网关、公网 LB 与 Internet 通信，通过对等连接与对端 VPC 通信。



# 网络性能大盘

最近更新时间：2024-03-20 17:08:41

网络性能大盘用于查看腾讯云支持的地域间以及地域内可用区间的内网延时情况，以便您实时了解网络性能，更好规划云上资源分布。

## 操作步骤

1. 登录 [私有网络控制台](#)。
2. 单击左侧导航中的网络性能大盘，进入网络性能大盘的展示界面。

## 地域间内网性能



**说明：**

源和目的地域交换前后的时延数据可能由于底层传输线路的不同而有差异。

选择地域，单击地域间连线可查看已选地域间的网络时延情况。

请选择要查看的地域

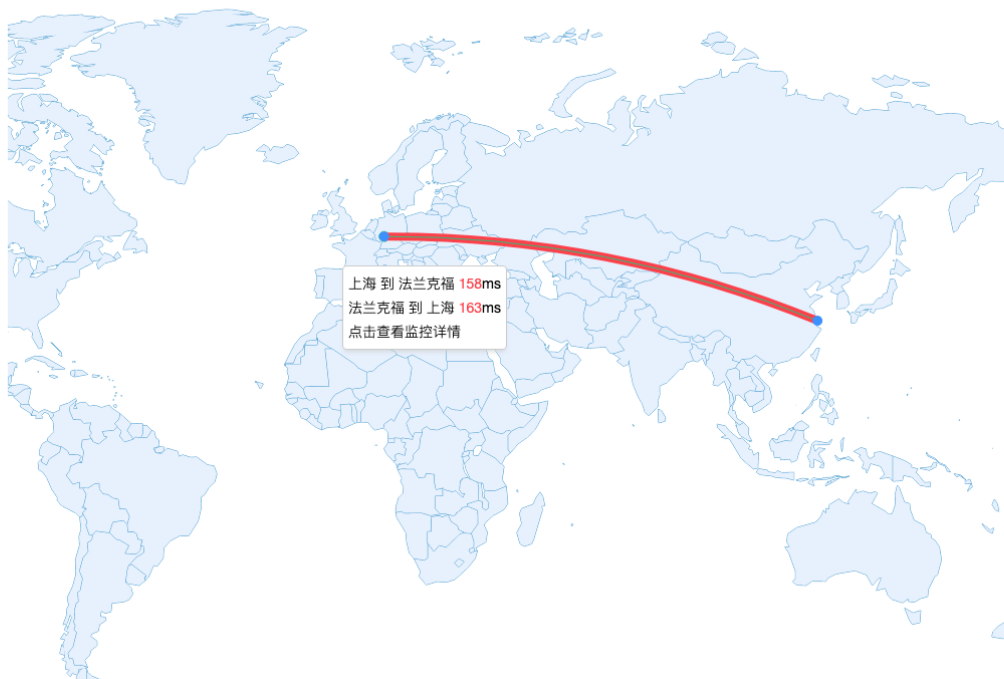
上海

X

法兰克福

X

添加地域



## 地域内内网性能

选择地域，可查看地域内可用区间的网络时延情况。

请选择要查看的地域

上海

暂不支持同一可用区间延时检测

上海一区	-	1.06ms	1.12ms	0.68ms	2.4ms	2.07ms
上海二区	1.18ms	-	1.73ms	0.91ms	1.19ms	1.33ms
上海三区	1.14ms	-	-	-	-	2.99ms
上海四区	-	0.92ms	1.3ms	-	1.94ms	1.58ms
上海五区	2.52ms	1.24ms	2.27ms	1.93ms	-	1.42ms
上海八区	2.15ms	1.37ms	3.09ms	1.6ms	1.44ms	-
	上海一区	上海二区	上海三区	上海四区	上海五区	上海八区

说明:

同一可用区无延时数据。



# 私有网络

## 概述

最近更新时间：2023-10-27 14:27:31

私有网络（VPC）是您在腾讯云上可以独享并可自主规划的一个完全逻辑隔离的网络空间，在使用云资源之前，您必须先创建一个私有网络和子网。子网是私有网络中的一个网络空间，私有网络具有地域属性，子网具有可用区属性，一个私有网络内至少包含一个子网，您可以在一个私有网络中创建多个子网来划分网络，同一私有网络中的子网默认内网互通。

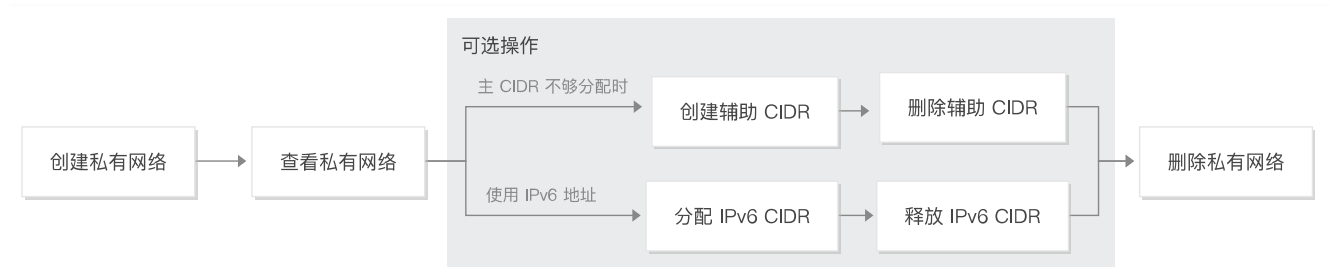
云服务器、负载均衡等云资源必须部署在子网内，不能直接部署在私有网络中。

本文将介绍 VPC 的使用生命周期。您可通过如下视频了解管理私有网络的相关信息。

[观看视频](#)

## 背景信息

根据不同的使用需求，VPC 的使用生命周期如下图所示：



- 创建私有网络**：创建 VPC 前，您需要提前做好 [网络规划](#)。VPC 和子网的 CIDR 创建后不可更改。
- 查看私有网络**：可查看 VPC 的基本信息、云联网的关联情况以及包含资源。
- （可选）根据实际使用场景选择不同操作：
  - 主 CIDR 不够分配时，参考 [编辑 IPv4 CIDR](#)：
    - 创建辅助 CIDR**：主 CIDR 不够分配时，可以创建辅助 CIDR 以满足实际网络需求。
    - 删除辅助 CIDR**：若不需要辅助 CIDR，可将其删除。
  - 若需使用 IPv6 地址，参考 [编辑 IPv6 CIDR](#)：
    - 分配 IPv6 CIDR**：若需使用 IPv6 地址，可以创建 IPv6 CIDR 以满足实际网络需求。
    - 释放 IPv6 CIDR**：如不需要 IPv6 CIDR，可将其释放。释放后，VPC 内所有云资源的 IPv6 地址都将被释放，且不可找回。
- 删除私有网络**：删除 VPC 后，该 VPC 下的子网和路由表将一并被删除。

## 限制说明

最近更新时间：2023-10-27 14:27:31

### 使用限制

- 私有网络和子网的网段创建后无法修改。
- 腾讯云保留了各个子网的前面两个 IP 地址和最后一个 IP 地址，以作 IP 联网之用。例如，子网 CIDR（无类别域间路由）为 172.16.0.0/24，则腾讯云保留的 IP 地址为：172.16.0.0、172.16.0.1 和 172.16.0.255。
- 向私有网络中添加云服务器时，系统会在指定子网内为该实例默认随机分配一个内网 IP，用户可以在云服务器创建后，重新指定每台云服务器的内网 IP。
- 在私有网络内，云服务器一个内网 IP 对应一个公网 IP。
- 基础网络云服务器不支持和辅助 CIDR 内的云资源互通。
- 对等连接不支持传递辅助 CIDR。

### 配额限制

资源	限制 / 个
每个账号每个地域内的私有网络个数	20
每个私有网络内的子网数	100
每个私有网络内辅助 CIDR 个数	5

#### 说明

如需提升配额，请提 [工单申请](#)。

# 创建私有网络

最近更新时间：2023-10-27 14:27:31

私有网络是使用云服务的基础，您可以参考本章节，在私有网络控制台新建私有网络。

## 操作指南

1. 登录 [私有网络控制台](#)。
2. 在私有网络页面顶部，选择 VPC 所属地域，单击新建。
3. 在弹出的新建 VPC 对话框中，填写 VPC 信息和初始子网信息。

### 说明

VPC 和子网的 CIDR 创建后不可修改。

- VPC CIDR 支持使用如下网段中的任意一个，如果您有不同 VPC 间内网通信的需要，请确保两端 VPC 的 CIDR 配置不要重叠：
  - 10.0.0.0 - 10.255.255.255（掩码范围需在12 - 28之间）
  - 172.16.0.0 - 172.31.255.255（掩码范围需在12 - 28之间）
  - 192.168.0.0 - 192.168.255.255（掩码范围需在16 - 28之间）
- 子网的 CIDR 必须在 VPC 的 CIDR 内或与之相同。  
例如，VPC 的网段是 10.0.0.0/16，那么该 VPC 内的子网的网段可以是 10.0.0.0/16、10.0.0.0/24 等。
- 可用区：子网具有可用区属性，请选择初始子网所在的可用区。同一私有网络下可以有不同可用区的子网，同一私有网络下不同可用区的子网默认可以内网互通。
- 关联路由表：子网必须关联一个路由表进行流量转发控制，初始子网关联的是一个默认路由表，该路由表由系统默认下发，表示 VPC 内网络互通。
- 标签：您可按需添加标签，帮助您更好地管理子用户、协作者的资源权限，非必选参数，可按需设置。

新建VPC

私有网络信息

所属地域 华南地区(深圳)

名称

不超过60个字符，允许字母、数字、中文字符、'-'、'\_'、'.'

IPv4 CIDR 10.0.0.0/16

网段创建后不可更改, 请您提前做好网络规划

标签 标签键 标签值

+ 添加

初始子网信息

子网名称

不超过60个字符，允许字母、数字、中文字符、'-'、'\_'、'.'

IPv4 CIDR 10.0.0.0/24

IP地址剩余253个

可用区 ① 请选择

关联路由表 默认 ①

标签 标签键 标签值

+ 添加

确定 关闭

4. 参数设置完成后，单击确定完成 VPC 的创建，创建成功的 VPC 展示在列表中，如下图所示，新建 VPC 包含一个初始子网和一个默认路由表。

私有网络 私有网络帮助文档

[+新建](#)

ID/名称	IPv4 CIDR	子网	路由表	NAT 网关	VPN 网关	云服务器	基础网络互通	专线网关	默认私有网络	创建时间	操作
vpc-45msitq4	172.16.0.0/16	1	1	0	0	0	0	0	否	2020-11-03 16:37:00	<a href="#">删除</a> <a href="#">更多</a>

## 后续操作

VPC 及初始子网创建成功后，即可在 VPC 中部署云资源，例如云服务器、负载均衡等。  
 可单击如下红框图标，直接跳转至云服务器购买页面进行购买，详情请参见 [快速搭建 IPv4 私有网络](#)。

ID/名称	IPv4 CIDR	IPv6 CIDR	组播	子网	路由表	NAT 网关	VPN 网关	云服务器	专线网关	默认私有网络	创建时间	操作
vpc-11...	11...:0(主)   1		<input type="checkbox"/>	2	2	1	0	23	1	否	2020-08-05 11:19:36	<a href="#">删除</a> <a href="#">更多</a>

## 相关内容

在私有网络中，有一个默认私有网络，即：  
 当一个地域未创建任何私有网络，在该地域创建云服务器、负载均衡或数据库时，您可以选择腾讯云为您自动创建默认私有网络和子网，而无需自行创建，如下图所示。

可用区: 随机可用区 成都一区 成都二区 ?

网络: vpc-... Def... ? 子网剩余可用IP 4093个

当前网络为默认私有网络/子网，建议您根据业务需要进行调整  
 如现有私有网络/子网不符合您的要求，可以去控制台 [新建私有网络](#) 或 [新建子网](#)。云服务器购买后可以通过控制台切换私有网络完成私有网络/子网的切换

实例创建成功后，一个默认的私有网络和子网也会随之创建成功，该默认私有网络和子网与您自行创建的私有网络和子网功能完全一致，且不占用您在某个地域下的配额，如果您不再需要可自行删除。一个地域只能有一个默认私有网络，一个可用区只能有一个默认子网。

网络拓扑 | [私有网络](#) | [子网](#) | [路由表](#) | [IP与网卡](#)

[+新建](#)

ID/名称	IPv4 CIDR	子网	路由表	NAT 网关	VPN 网关	云服务器	基础网络互通	专线网关	默认私有网络	创建时间	操作
Default-VPC	172.16.0.0/16	1	1	0	0	0	0	0	是	2020-12-16 17:01:42	<a href="#">删除</a> <a href="#">更多</a>

[+新建](#) 筛选

ID/名称	所属网络	CIDR	可用区	关联路由表	云服务器	可用IP	默认子网	创建时间	操作
sub-Def...	vpc-Def...	172.16.0.0/16	广州西区	rtb-def...	0	4093	是	2021-01-26 22:28:02	<a href="#">删除</a> <a href="#">更多</a>

# 查看私有网络

最近更新时间：2024-03-20 17:08:41

私有网络控制台提供所有 VPC 的资源查询功能，包括 VPC 内的云资源、以及网络连接等。

## 操作指南

1. 登录 [私有网络控制台](#)。
2. 在私有网络页面顶部，选择 VPC 所属地域，在 VPC 列表中，可查看该地域下所有的 VPC，其中界面展示的列表字段含义如下。



字段	字段含义
ID/名称	私有网络 VPC 的 ID 和名称，名称支持修改。
IPv4 CIDR	VPC 的 IPv4 CIDR，不支持修改。
IPv6 CIDR	VPC 的 IPv6 CIDR，IPv6 目前还在内测中，如需使用，需提交 <a href="#">内测申请</a> 。
子网	该 VPC 中包含子网的个数，单击数目可进入子网界面。
路由表	该 VPC 中包含的路由表个数，单击数目可进入路由表界面。
NAT 网关	该 VPC 中包含的 NAT 网关的个数，单击数目可进入 NAT 网关界面。
VPN 网关	该 VPC 中包含的 VPN 网关的个数，单击数目可进入 VPN 网关界面。
云服务器	该 VPC 中包含的云服务器的个数，单击数目可进入云服务器界面，单击云服务器图标可跳转至云服务器购买页面。
专线网关	该 VPC 中包含的专线网关的个数，单击数目可进入专线网关界面。
默认私有网络	表示该 VPC 是否为默认私有网络，一个地域只能有一个默认私有网络，该默认私有网络是在云服务器等云资源购买时，选择由腾讯云自动创建的默认私有网络和子网，其功能与用户自行创建的私有网络 VPC 是一样的。
创建时间	VPC 创建时间。
标签	该 VPC 所绑定的标签个数，鼠标悬停于该图案可展示详细内容。
操作	该 VPC 可执行的操作，只有无任何资源的 VPC 才可执行删除操作；更多中可以编辑 IPv4 CIDR 和 IPv6 CIDR。

3. 单击需要查看的 VPC ID，详情页中展示了 VPC 的基本信息、云联网的关联情况以及包含资源，单击资源数目，可进入相应的资源管理界面。

### 基本信息

IPv4 CIDR: 10.0.0.0/16 (主)

IPv6 CIDR: -

DNS: 10.0.0.100

Domain Name: -

标签: 无

### 关联云联网

云联网ID: vpc-2pmhix62

云联网名称: lucian-test-2

所属帐号: 我的帐号

状态: 已连接

关联时间: 2021-01-05 15:39:29

[解关联](#)

### 包含资源

基础云资源

- 云服务器: 1个
- 负载均衡: 0个

网络资源

- 子网: 2个
- 路由表: 1个
- 弹性网卡: 1个
- 对等连接: 0个
- 基础网络互通: 0个
- NAT网关: 0个
- VPN网关: 0个
- 专线网关: 1个
- 流日志: 0个
- 网络探测: 0个
- 网络ACL: 0个

其它云资源

- MySQL: 1个

4. 返回 VPC 界面，单击右上方的搜索框，支持按照不同资源属性进行过滤，快速查看指定 VPC。

私有网络 北京 73

私有网络帮助文档

私有网络API 已全面升级至3.0版本，基于2.0版本接口访问时延较高和使用复杂的考虑，原私有网络API 2.0 接口服务将不再提供技术支持，并将于2023年3月31日起下线。如果您的业务还在使用私有网络 API 2.0 相关接口，建议尽快将服务升级至API 3.0 接口，以免对您的业务造成影响。具体迁移指引详见《私有网络API2.0切换API3.0指引》。

新建

请输入私有网络 ID/名称

选择资源属性进行过滤

ID/名称	IPv4 CIDR	IPv6 CIDR	子网	路由表	NAT 网关	VPN 网关	默认私有网络	创建时间	标签	操作
vpc-2pmhix62 lucian-test-2	10.0.0.0/16	-	1	1	0	0	否	2023-07-20 19:11:21		删除 更多
vpc-bi8rsw4 lucian-test-1	10.0.0.0/16	-	2	2	0	0	否	2023-07-18 19:06:33		删除 更多

5. 单击设置图标，可自定义列表字段。

私有网络 北京 73

私有网络帮助文档

私有网络API 已全面升级至3.0版本，基于2.0版本接口访问时延较高和使用复杂的考虑，原私有网络API 2.0 接口服务将不再提供技术支持，并将于2023年3月31日起下线。如果您的业务还在使用私有网络 API 2.0 相关接口，建议尽快将服务升级至API 3.0 接口，以免对您的业务造成影响。具体迁移指引详见《私有网络API2.0切换API3.0指引》。

新建

请输入私有网络 ID/名称

ID/名称	IPv4 CIDR	IPv6 CIDR	子网	路由表	NAT 网关	VPN 网关	云服务器	专线网关	默认私有网络	创建时间	标签	操作
-------	-----------	-----------	----	-----	--------	--------	------	------	--------	------	----	----

6. 单击刷新图标，可刷新当前信息展示表。

7. 单击下载图标，可下载当前展示的所有信息。

## 编辑 IPv4 CIDR

最近更新时间：2023-10-27 14:27:31

VPC 支持添加一个主 CIDR，且主 CIDR 创建后不可更改，当主 CIDR 不满足业务分配时，您可以创建辅助 CIDR 来扩充网段，一个 VPC 支持添加多个辅助 CIDR。

子网支持从主 CIDR 或者辅助 CIDR 中分配网段，无论子网属于主 CIDR 还是辅助 CIDR，同一 VPC 下不同子网均默认互通。

### 使用限制

- 基础网络云服务器不支持和辅助 CIDR 内的云资源互通。
- 对等连接不支持传递辅助 CIDR。
- 云联网、VPN 网关、标准型专线网关支持传递辅助 CIDR，其中专线网关还存在如下限制：
  - 金融云地域的标准型专线网关不支持传递辅助 CIDR。
  - 标准型专线网关支持传递10个辅助 CIDR。
  - NAT 型专线网关不支持传递辅助 CIDR。

### 创建辅助 CIDR

- 登录 [私有网络控制台](#)。
- 在私有网络页面顶部，选择 VPC 所属地域。
- 在 VPC 列表中目标 VPC 右侧操作列选择更多 > 编辑 IPv4 CIDR。

ID/名称	IPv4 CIDR	IPv6 CIDR	子网	路由表	NAT 网关	VPN 网关	云服务器	基础网络...	专线网关	默认私有...	创建时间	操作
vpc-0mei4azr vpc-ε	10.10.10.0/ 24	-	3	1	0	0	2	0	0	否	2021-01-28 10:26:22	删除 更多

- 在弹出编辑对话框中单击添加，并编辑辅助 CIDR。

#### 注意

辅助 CIDR 可以和自定义路由的目的网段重叠，但需要谨慎操作，因为辅助 CIDR 的路由属于 Local 路由，Local 路由比自定义子网路由优先级更高。

编辑IPv4 CIDR

私有网络 vpc-ε

IPv4 CIDR 10.10.10.0/24主

172 . 16 . 0.0 / 16 删除

添加 ⓘ

确定 关闭

- 单击确定完成辅助 CIDR 的创建。

### 删除辅助 CIDR

- 登录 [私有网络控制台](#)。
- 在私有网络页面顶部，选择 VPC 所属地域。

- 在 VPC 列表中，待删除辅助 CIDR 的 VPC 右侧操作列选择更多 > 编辑 IPv4 CIDR。
- 在弹出的编辑对话框中，单击辅助 CIDR 后的删除。



- 单击确定完成删除操作。



## 编辑 IPv6 CIDR

最近更新时间：2023-10-27 14:27:31

VPC 支持 IPv6 功能，当您有 IPv6 业务需求时，需要先将 VPC 分配一个 IPv6 CIDR 网段，然后 VPC 内云资源才可以在 VPC 的 IPv6 CIDR 内分配到 IPv6 地址，从而进行 IPv6 业务通信。本章节介绍如何通过控制台为 VPC 分配 IPv6 CIDR。

### 说明

目前 IPv6/IPv4 双栈 VPC 功能处于内测中，如有需要，请提交 [内测申请](#)。

## 分配 IPv6 CIDR

1. 登录 [私有网络控制台](#)。
2. 在私有网络页面顶部，选择 VPC 所属地域。
3. 在 VPC 列表中，单击目标 VPC 右侧操作列选择更多 > 编辑 IPv6 CIDR。

ID/名称	IPv4 CIDR	IPv6 CIDR	子网	路由表	NAT 网关	VPN 网关	云服务器	基础网络...	专线网关	默认私有...	创建时间	操作
vpc-0mei4azrr-vpc-a	10.10.10.0/24	-	3	1	0	0	2	0	0	否	2021-01-28 10:26:22	删除 更多
vpc-qdx-vpc-...	10.0.0.0/16	-	1	1	0	0	4	0	0	否	2021-01-25 17:55:38	编辑IPv4 CIDR 编辑IPv6 CIDR

4. 在弹出的编辑对话框中单击获取，系统将为该 VPC 分配1个 /56 的 IPv6 CIDR。

### 编辑IPv6 CIDR

私有网络 vpc-e

IPv6 CIDR [获取](#)

每个VPC支持1个IPv6 CIDR，对等连接、专线等场景暂不支持IPv6通信

[确定](#) [关闭](#)

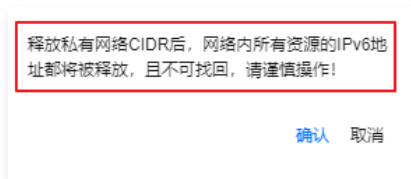
5. 单击确定完成 IPv6 CIDR 分配。

## 释放 IPv6 CIDR

1. 登录 [私有网络控制台](#)。
2. 在私有网络页面顶部，选择 VPC 所属地域。
3. 在 VPC 列表中已获取 IPv6 CIDR 的 VPC 右侧操作列选择更多 > 编辑 IPv6 CIDR。
4. 在弹出的 IPv6 CIDR 编辑对话框中，单击释放。



5. 在弹出的风险提示框中，知悉释放操作的风险并确认无误后，单击确认完成 IPv6 CIDR 释放。



## 修改私有网络 DNS 信息

最近更新时间：2023-10-27 14:27:32

腾讯云私有网络内的云服务器支持 DHCP 协议，支持配置的 DHCP Options 字段包括：DNS 地址、Domain Name。本文将介绍如何修改 VPC 网络的 DNS 地址、Domain Name 信息。

### 说明

- 动态主机设置协议（Dynamic Host Configuration Protocol, DHCP）是一种局域网的网络协议，提供了将配置信息传递到 TCP / IP 网络服务器的标准。
- 2018年4月1日前创建的私有网络暂不支持 DHCP 特性，若您在控制台无法修改 DNS 地址和 Domain Name，即说明您的私有网络不支持该特性。

### 注意事项

配置修改后，对该私有网络内所有云服务器生效：

- 新建的云服务器：直接生效。
- 存量的云服务器：重启云服务器或重启网络服务生效。

### 操作步骤

- 登录 [私有网络控制台](#)。
- 在私有网络页面顶部，选择 VPC 所属地域。
- 单击 VPC ID，进入 VPC 详情的基本信息界面。
- 分别单击如下编辑图标，可修改 DNS、Domain Name。
  - DNS：DNS 服务器地址。

### 说明

- 腾讯云默认 DNS 地址为：183.60.83.19，183.60.82.98，如果不使用腾讯云默认 DNS，将无法使用内部服务，如 Windows 激活、NTP、YUM 等。
- 目前 DNS 最多支持4个 IP，多个 IP 之间请用英文逗号隔开，但某些操作系统可能无法支持4个 DNS 地址。

- Domain Name：云服务器 hostname 后缀，例如 `example.com`。最多支持60个字符，如无特殊需求，也可保持默认。



## 修改私有网络名称和标签

最近更新时间：2023-10-27 14:27:32

本文将介绍如何修改 VPC 名称、标签等信息。

### 操作步骤

1. 登录 [私有网络控制台](#)。
2. 在私有网络页面顶部，选择 VPC 所属地域。
3. 单击 VPC 名称旁的编辑图标，可对 VPC 的名称进行修改。



4. 单击 VPC ID，进入 VPC 详情的基本信息界面。
5. 标签主要用于资源标识，以便后期管理，单击如下编辑图标，可修改标签内容，请根据实际情况选择设置，支持增、删多条标签。



# 关联或解关联云联网

最近更新时间：2023-11-23 10:40:11

云联网可提供云上 VPC 间、VPC 与 IDC 间多点内网互联服务，如需使用云联网打通 VPC 与 VPC、VPC 与 IDC 间的通信，首先需要将 VPC 关联到云联网实例上。本章节介绍如何为 VPC 关联/解关联云联网。

## 关联云联网

1. 登录 [私有网络控制台](#)。
2. 在私有网络页面顶部，选择 VPC 所属地域。
3. 单击 VPC ID 进入 VPC 详情中**基本信息**页面。
4. 单击**关联云联网**区域下的**立即关联**，进入关联云联网对话框。

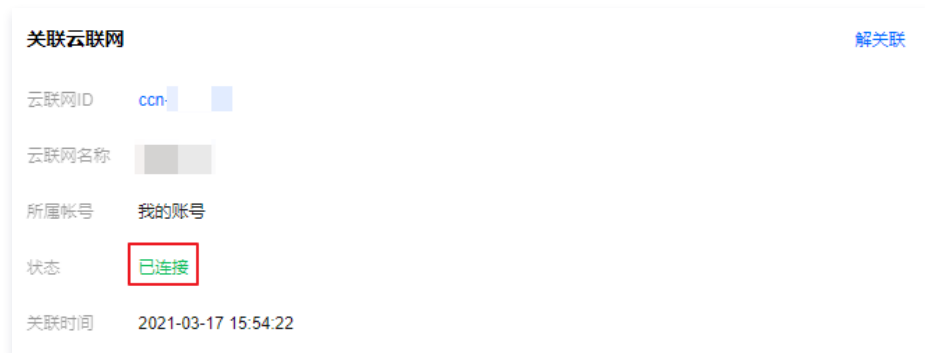


5. 配置关联云联网的如下参数。



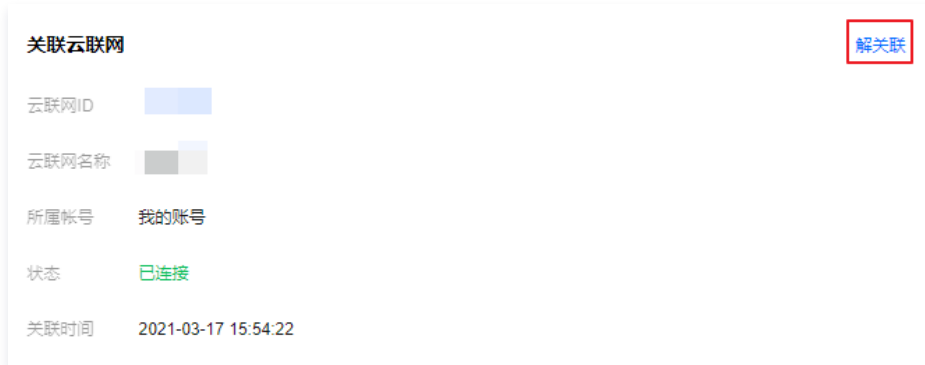
- **所属帐号**：待关联云联网实例所属帐号，支持将 VPC 关联到同帐号或跨帐号下的云联网实例上。如选择**其他帐号**，则需要提前获取到对方的帐号 ID，且申请关联后，对方需在7天内同意此次申请，否则关联申请将过期。实例加入云联网产生的网络互通费用，由云联网所在帐号承担。
- **云联网**：如所属帐号为**我的帐号**，请在下拉框中选择具体的云联网实例 ID。如所属帐号为**其他帐号**，请提前获取对方帐号下的待关联云联网 ID，并填写。

6. 单击**确定**完成关联操作，VPC 成功关联到云联网实例后，状态为**已连接**。

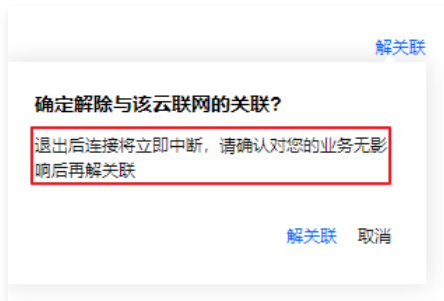


## 解关联云联网

1. 登录 [私有网络控制台](#)。
2. 在私有网络页面顶部，选择 VPC 所属地域。
3. 单击待解关联云联网的 VPC ID 进入 VPC 详情中基本信息页面。
4. 单击关联云联网区域下的解关联。



5. 在风险提示框中，充分知悉操作风险，确认无误后，单击解关联完成操作。



## 相关操作

- [同帐号网络实例互通](#)
- [跨帐号网络实例互通](#)

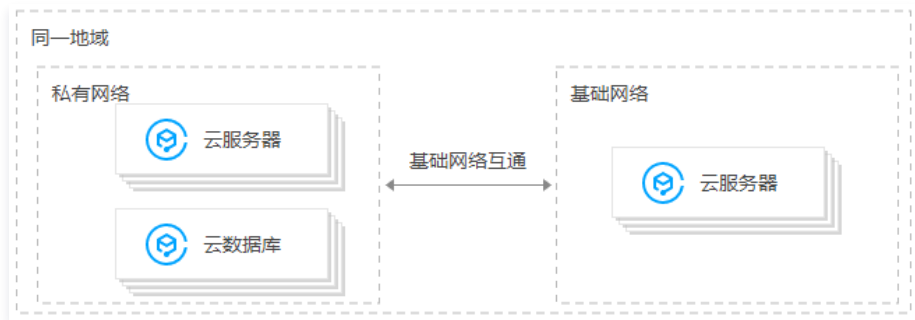
# 基础网络互通

## 概述

最近更新时间：2023-03-30 19:22:06

基础网络互通实现私有网络与基础网络服务器的通信。通过基础网络互通可实现如下通信场景：

- 基础网络中的云服务器可以访问私有网络中的云服务器、云数据库、内网负载均衡、云缓存等云资源。
- 私有网络内的云服务器，只能访问互通的基础网络云服务器，无法访问基础网络中云数据库、负载均衡等其他云资源。



### 使用限制

- 仅支持同地域下的私有网络与基础网络互通。
- 仅当私有网络的网段在10.0.0.0/16 – 10.47.0.0/16（含子集）范围内时，才可与基础网络建立互通，如果您的私有网络网段不在此范围内，可能会与基础网络IP段冲突，导致无法关联基础网络云服务器，进而无法与基础网络云服务器通信。
- 1个基础网络云服务器同一时间只能关联1个私有网络。
- 1个私有网络最多支持关联100台基础网络云服务器。
- 基础网络云服务器关联到某个私有网络后，仅支持与私有网络主CIDR的资源通信，不支持与私有网络辅助CIDR的资源通信。
- 私有网络中的负载均衡实例，不能绑定与本私有网络互通的基础网络云服务器。
- 基础网络互通中，云服务器的流量只能路由至私有网络中的内网IP地址，无法路由至私有网络以外的其他目标。

#### 说明

即基础网络云服务器，不能经由本私有网络的VPN网关、专线网关、公网网关、对等连接、NAT网关等网络设备，访问本私有网络外的公网或私网资源。同样VPN网关、专线网关、对等连接等网络设备的对端，也无法访问本基础网络的云服务器。

### 注意事项

- 基础网络云服务器内网IP的变更，将导致私有网络关联失效，即原记录将失效。如需关联，请重新在私有网络控制台进行添加。
- 基础网络云服务器欠费隔离、安全隔离、冷迁移、故障迁移、修改配置、切换操作系统等操作均不会解绑与私有网络的互通关系。
- 基础网络云服务器退还后，将自动解绑与私有网络的互通关系。

### 相关文档

基础网络互通相关操作，请参见 [管理基础网络互通](#)。

## 管理基础网络互通

最近更新时间：2023-07-24 18:33:42

### 创建基础网络互通

通过将基础网络云服务器关联到某私有网络，从而建立私有网络与基础网络的互通功能，使得基础网络云服务器可以与私有网络内资源通信。

#### ① 说明

- 关联私有网络后的基础网络云服务器内网 IP，会自动添加至私有网络路由表的 Local 策略中，您无需手动修改当前私有网络的路由表策略，即可以实现互访。
- 基础网络内云服务器与私有网络关联后，各自的安全组与网络 ACL 仍然有效。

### 操作步骤

1. 登录 [私有网络控制台](#)。
2. 选择地域，单击需要与基础网络互通的 TomVPC 的 ID，进入详情页。

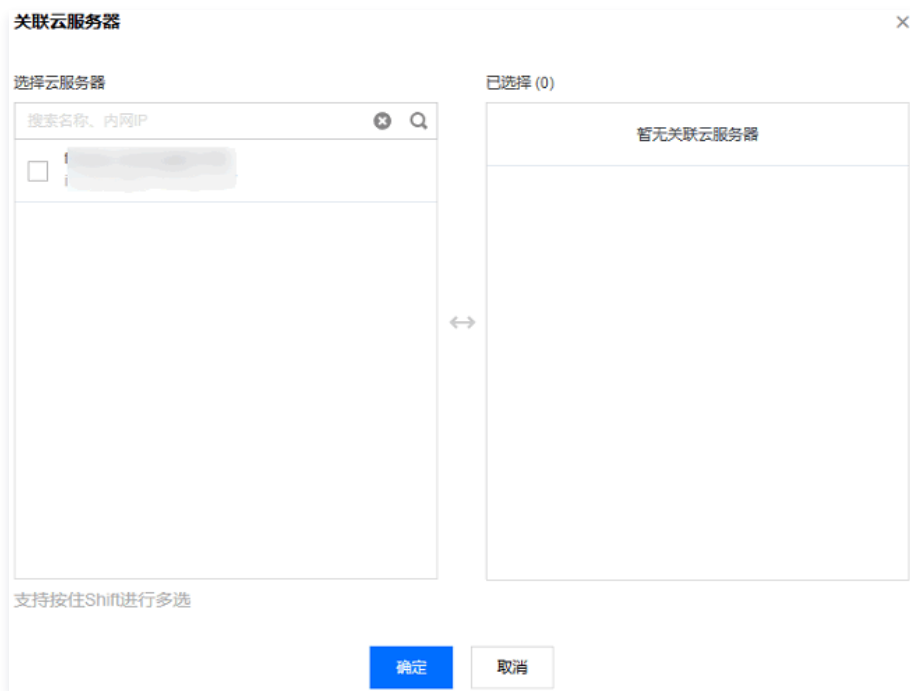
#### ① 说明

本场景中，用户所属的 VPC 网络为 TomVPC。

3. 单击基础网络互通选项卡，单击+关联云服务器。



4. 在弹出框中，选择基础网络内需要关联至此私有网络的云服务器，例如 TomCVM，单击确定即可。



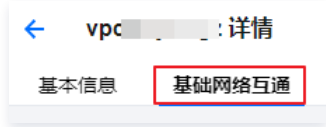
### 查看基础网络互通



可查看所有与私有网络互通的基础网络云服务器列表。

### 操作步骤

1. 登录 [私有网络控制台](#)。
2. 选择地域，单击需要与基础网络互通的 VPC ID，进入详情页。
3. 单击**基础网络互通**选项卡，即可查看与该私有网络关联的基础网络云服务器列表。



4. 在右上方的搜索框内，支持按照云服务器内网 IP 进行快速搜索。

### 删除基础网络互通

通过将基础网络云服务器与私有网络解关联操作，可删除私有网络与基础网络的互通功能。

### 操作步骤

1. 登录 [私有网络控制台](#)。
2. 单击需要删除基础网络互通的 VPC ID，进入 VPC 详情页。
3. 单击**基础网络互通**选项卡，在基础网络云服务器列表中，找到需要解关联的云服务器，单击操作栏中的**解关联**。



4. 确认操作无误后，单击**确定**完成解关联即可。
5. 如需批量解关联，可勾选云服务器列表，然后单击上方的**解除关联**进行批量解关联操作。

# 开启或关闭组播功能

最近更新时间：2023-03-21 11:04:31

本章节介绍私有网络维度的组播功能的开启与关闭。

## 背景信息

组播和广播是一对多的通信方式，通过单点到多点的高效数据传送，可以为企业节约网络带宽、降低网络负载。

如果使用单播技术，发送主机需要分别向 N 个主机发送，共发送 N 次；如果使用组播和广播，主机向 N 个主机发送相同的数据时，只要发送1次，既节省服务器资源，也节省了网络主干的带宽资源。

### 说明

- 内测申请已结束，公测敬请期待！
- 目前支持组播和广播的地域为：北京、上海、广州、成都、重庆、南京、中国香港、新加坡、首尔、东京、曼谷、多伦多、硅谷、弗吉尼亚、法兰克福、深圳金融、上海金融、北京金融。
- 单 VPC 组播、广播最大支持5万 pps、190Mbps。

- 组播：腾讯云支持私有网络维度的组播。
- 广播：腾讯云支持子网维度的广播。

## 操作场景

组播和广播较多应用于金融和游戏行业：

- 金融行业主要用于广播业务或行情数据。例如，获取股票价格等实时数据时，券商可通过广播，对多台 client 实时发送股票数据，有效降低网络负载。
- 游戏行业主要用于多台服务器之间的心跳保持。

## 操作步骤

### 开启组播

1. 登录 [私有网络控制台](#)。
2. 在列表中，找到需要开启组播功能的私有网络所在行，单击组播下的开启并确认操作即可。



### 关闭组播

1. 登录 [私有网络控制台](#)。
2. 在列表中，找到需要关闭组播功能的私有网络所在行，单击组播下的关闭并确认操作即可。

私有网络 广州

[+新建](#)

ID/名称	IPv4 CIDR	IPv6 CIDR	组播	子网	路由表	NAT 网关
vp	10		<input checked="" type="checkbox"/>	2	2	1

### 相关操作

子网维度的广播功能的操作指导请参考 [开启或关闭广播](#)。

## 删除私有网络

最近更新时间：2024-04-22 10:18:21

当 VPC 不再使用，且 VPC 中除空子网、路由表、网络 ACL 之外，没有其他资源（对等连接、基础网络互通、NAT 网关、VPN 网关、专线网关、云联网、私有连接等）时，可删除 VPC。

### 说明

- 空子网是指子网内无 IP 占用，即当私有网络内只有空子网、路由表和网络 ACL 时，可以删除私有网络；当子网内有 IP 占用时，无法删除私有网络。
- 如您在操作删除私有网络过程中还存在其它问题，可通过 [提交工单](#) 获取帮助。

### 操作步骤

- 登录 [私有网络控制台](#)。
- 在私有网络页面顶部，选择 VPC 所属地域。
- 在 VPC 列表中待删除的 VPC 右侧操作列单击删除，并确认操作。

ID/名称	IPv4 CIDR	IPv6 CIDR	子网	路由表	NAT 网关	VPN 网关	云服务器	基础网络...	专线网关	默认私有...	创建时间	操作
vpc-r52t	10.0.0.0/24	-	3	2	0	0	0	0	1	否	2020-03-24 21:52:45	删除 更多
vpc-17	10.0.0.0/24	-	0	1	0	0	0	0	0	否	2020-03-24 19:23:45	删除 更多

# 子网

## 创建子网

最近更新时间：2024-03-19 10:05:51

子网是私有网络的一个网络空间，云资源部署在子网中。一个私有网络中至少有一个子网，因此在创建私有网络时，会同步创建一个初始子网。当您有多业务需要部署在不同子网，或已有子网不满足业务需求时，您可以在私有网络中继续创建新的子网。

子网具有可用区属性，同一私有网络下可以创建不同可用区的子网，同一私有网络下不同可用区的子网默认可以内网互通。本章节提供在私有网络中创建子网的操作指导。

### 操作步骤

1. 登录 [私有网络控制台](#)。
2. 在左侧目录中单击子网，进入管理页面。
3. 选择需要创建子网的地域和私有网络，单击**新建**。
4. 在弹出的**创建子网**对话框中，配置子网参数。

子网名称	VPC网段	CIDR	可用区	关联路由表	操作
请输入子网名称	10.0.0.0/24	10.0.0.0/24	广州二区	default	-
请输入子网名称	10.0.0.0/24	10.0.0.0/24	广州三区	default	✕

- **所属网络**：子网所在的私有网络，如果 [步骤3](#) 中已选择私有网络，则此处自动显示已选择的私有网络，如 [步骤3](#) 中未选择私有网络，则可以在下拉箭头中选择子网所在的私有网络。
- **子网名称**：自定义子网名称，字符长度在60个以内。
- **VPC网段**：此处自动展示已选择的私有网络的 CIDR。
- **CIDR**：设置子网的 CIDR。子网的 CIDR 必须是所在私有网络 CIDR 的一部分，且不能和该私有网络下已有子网的 CIDR 重叠。

#### 说明

请根据实际业务规模规划子网的网段范围，在创建云服务实例时，系统会在指定子网内为该实例默认随机分配一个内网 IP，云服务器主内网 IP 支持修改，详情可参考 [修改主内网 IP](#)。

- **可用区**：选择子网所在的可用区。
  - **关联路由表**：选择子网需要关联的路由表，子网必须关联一个路由表来控制出流量的走向。子网默认关联的是私有网络内的默认路由表，该路由表由系统默认下发，表示 VPC 内网络互通，也可选择该私有网络内的其他路由表。
  - **新增一行**：用户可以创建一个或多个子网。单击**新增一行**可以同时创建多个子网，单击✕可以删除子网。
  - **标签**：此处可以设置子网的标签信息，标签信息有利于子网资源的管理，可按需设置，如需设置多个，可单击**添加**，如需删除请单击操作列的删除图标。
5. 参数设置完成后，单击**创建**即可，创建成功的子网展示在列表中，如下图所示。

子网 广州 全部私有网络 查看 API Inspector x 子网帮助文档

+新建 筛选 多个关键字用竖线“|”分隔，多个过滤标签用回车键分隔

ID/名称	所属网络	CIDR	IPv6 CIDR	可用区	关联路由表	云服务器	可用IP	默认子网	创建时间	操作
sub-	vpc-	10.0.0.0/20	-	广州六区	rtb-	5	4086	是	2020-11-12 16:20:16	删除 更多
sub-	vpc-	10.0.0.0/24	-	广州三区	rtb-	5	220	否	2020-10-29 12:33:01	删除 更多
sub-	vpc-	10.0.0.0/28	2400:0000:0000:0000::/24	广州一区	rtb-	0	11	否	2020-08-05 11:22:51	删除 更多

### 后续操作

子网创建成功后，即可在子网中部署云资源，例如云服务器、负载均衡等。

可单击如下红框图标直接跳转至云服务器购买页面进行购买，详情请参见 [快速搭建 IPv4 私有网络](#)。

ID/名称	IPv4 CIDR	IPv6 CIDR	组播	子网	路由表	NAT 网关	VPN 网关	云服务器	专线网关	默认私有...	创建时间	操作
vpc-	10.0.0.0/24 主   1		<input type="checkbox"/>	2	2	1	0	23 	1	否	2020-08-05 11:19:36	删除 更多

## 查看子网

最近更新时间：2023-10-27 14:27:32

私有网络控制台提供 VPC 下所有子网的资源查询功能，例如部署在子网中的云资源，子网关联的路由表、子网绑定的 ACL 规则等。

### 操作步骤

1. 登录 [私有网络控制台](#)。
2. 在左侧目录中单击子网，进入子网管理页面。
3. 在子网页面顶部，选择子网所属地域和所属 VPC，如果保持默认的全部私有网络，则可查看该地域下所有 VPC 下的所有子网，如下图所示。

#### 说明

- 单击子网界面所属网络的 VPC ID、关联路由表的路由表 ID 也可查看相应资源的详细信息。
- 单击云服务器的数目，可进入云服务器列表界面，如数目为0，可单击云服务器图标跳转至购买页。
- 单击子网展示界面字段的可用区，可查看指定可用区下的子网列表。
- 单击右上方的搜索框，可根据子网 ID、子网名称、标签、关键字、IPv4 CIDR 属性进行快速搜索。
- 单击右上方的设置图标，可自定义界面显示字段。

ID名称	所属网络	CIDR	IPv6 CIDR	可用区	关联路由表	子网广播	云服务器	可用IP	默认子网	创建时间	标签	操作
subne...	vpc...	10...	-	深圳一区	rtb...	☐	0	253	否	2023-02-28 13:08:51		删除 更多
subl...	vpc...	10...	-	深圳一区	rtb...	☐	0	248	否	2022-07-04 19:59:58		删除 更多

其中界面展示的列表字段含义如下：

- **ID/名称**：显示子网 ID 和名称。每个子网在创建时，系统都会分配一个 ID，子网名称支持实时修改。
  - **所属网络**：子网所属的 VPC 网络。
  - **CIDR**：子网的 CIDR 网段，子网 CIDR 不支持修改。
  - **可用区**：展示子网所在的可用区。
  - **关联路由表**：子网关联的路由表。
  - **云服务器**：显示子网中部署的云服务器个数。
  - **可用 IP**：子网 CIDR 范围内，可用的 IP 地址个数。
  - **默认子网**：在私有网络及子网控制台由用户自行创建的子网，均为非默认子网，此处显示为否；如果是在云服务器购买页面，选择由腾讯云自动创建的默认私有网络和子网，那么此处显示为是，一个地域只能有一个默认私有网络和子网。
  - **创建时间**：子网创建时间。
  - **标签**：您可按需添加标签，帮助您更好地管理子用户、协作者的资源权限。
  - **操作**：子网可执行的操作。无资源的子网，可执行删除操作；**更多** > **更换路由表**可更换子网关联的路由表。
4. 单击子网 ID 可查看子网包含的资源详情，切换页签可查看路由策略、ACL 规则。

← su [redacted] 详情

**基本信息** 路由策略 ACL规则

**基本信息**

子网名称	De [redacted]
子网ID	su [redacted]
子网CIDR	17 [redacted] /20
IPv6 CIDR	-
所属网络	vpc [redacted] (De [redacted] 16)
地域	广州
可用区	广州六区
关联ACL	无 <a href="#">绑定</a>
默认子网	是
标签	无 <a href="#">+</a>
创建时间	2020-11-12 16:20:16



# 获取与释放 IPv6 CIDR

最近更新时间：2023-10-27 14:27:32

当您的私有网络有 IPv6 业务通信需求时，您需要先为网络环境配置 IPv6 网段，然后才能在 VPC 内的资源分配 IPv6 地址，从而进行 IPv6 通信业务。大致顺序为：获取 VPC IPv6 CIDR > 获取子网 IPv6 CIDR > 云资源实例分配 IPv6 地址。本章节为您介绍子网 IPv6 CIDR 的获取与释放。

## 说明

目前 IPv6/IPv4 双栈 VPC 功能处于内测中，如有需要，请提交 [内测申请](#)。

## 获取 IPv6 CIDR

### 前提条件

子网所属的 VPC 已获取 IPv6 CIDR。

### 操作步骤

1. 登录 [私有网络控制台](#)。
2. 在左侧目录中单击子网，在子网列表上方，选择地域和私有网络，将会展示所属地域和私有网络下的所有子网信息。
3. 选择一个子网，单击操作列的更多 > 获取 IPv6 CIDR。



4. 填写如下 IP 段，范围为 0~255，请确认不能与其他子网的 IPv6 CIDR 网段重叠，单击确认系统将为该子网分配1个 /64 的 IPv6 CIDR。



### 相关文档

[搭建 IPv6 私有网络](#)

### 释放IPv6 CIDR

1. 登录 [私有网络控制台](#)。
2. 在左侧目录中单击子网，在子网列表上方，选择地域和私有网络，将会展示所属地域和私有网络下的所有子网信息。
3. 选择一个已获取到 IPv6 CIDR 的子网，更多 > 释放 IPv6 CIDR。

subr NAT	vpc hen	10.0.0.0/28	240.0.0.0/24	广州一区	rtb-1	0	11	公网	2020-08-05 11:22:51	删除 <b>更多</b>
<div style="border: 1px solid #ccc; padding: 2px;"> <a href="#">更换路由表</a>  <a href="#">释放IPv6 CIDR</a> </div>										
subt	vp To	10.0.0.0/18	-	广州一区	rt	0	16381	公网	2020-07-31 18:15:21	

4. 在弹出的确认框中，单击**确定**，系统将回收该子网的 IPv6 CIDR。

子网 华南地区 (广州) 全部私有网络 私有网络与子网帮助文档

+新建

ID/名称	所属网络	IPv4 CIDR	IPv6 CIDR	可用区	关联路由表	子网广播	云服务器	可用IP	默认子网	操作
		10.0.0.0/28	240.0.0.0/24	广州三区		<input type="checkbox"/>	5	4086	是	<a href="#">释放IPv6</a> <div style="border: 1px solid #ccc; padding: 5px; width: fit-content;"> <p>您确定要释放子网(s)的IPv6 CIDR?</p> <p style="text-align: right;"> <a href="#">确定</a> <a href="#">取消</a> </p> </div>

# 更换子网路由表

最近更新时间：2023-10-27 14:27:32

每个子网都必须关联一个 [路由表](#)，用于控制子网出流量的走向。子网关联的路由表支持实时更换，可根据业务实际情况，在子网控制台进行路由表的更换。如需新建路由表，请参见 [创建自定义路由表](#)。

## 对系统的影响

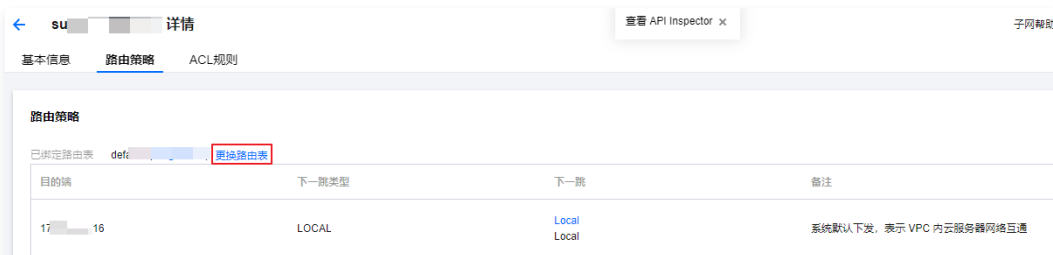
更换子网路由表会导致该子网下所有实例启动新的路由表策略，请仔细评估业务影响。

## 操作步骤

1. 登录 [私有网络控制台](#)。
2. 在左侧目录中单击子网，进入子网管理页面。
3. 更换子网关联的路由表，系统提供两种方式：
  - 单击待更换路由表的子网右侧操作列的 **更多** > **更换路由表**。



- 单击待更换路由表的子网 ID，进入详情页签，切换至 **路由策略** 页签，单击 **更换路由表**。



4. 在弹出的 **更换路由表** 对话框中，单击下箭头选择路由表，并知悉更换路由表的业务影响，确认无误后单击 **确认** 完成更换。



## 管理 ACL 规则

最近更新时间：2023-10-27 14:27:32

**ACL 规则** 是一种子网级别的可选安全层，用于控制进出子网的数据流，可以精确到协议和端口粒度，实现子网粒度流量的精细化控制。您可以为具有相同网络流量控制的子网关联同一个网络 ACL。

本章节介绍通过子网控制台绑定、解绑、更换 ACL 规则的操作指导。

### 操作步骤

1. 登录 [私有网络控制台](#)。
2. 在左侧目录中单击子网，进入子网管理页面。
3. 单击某子网 ID，进入子网详情界面后，可选择在如下任一位置执行 ACL 的绑定、解绑、更换操作。

- 在基本信息页签下的**关联 ACL**中



- 在 **ACL 规则** 页签下

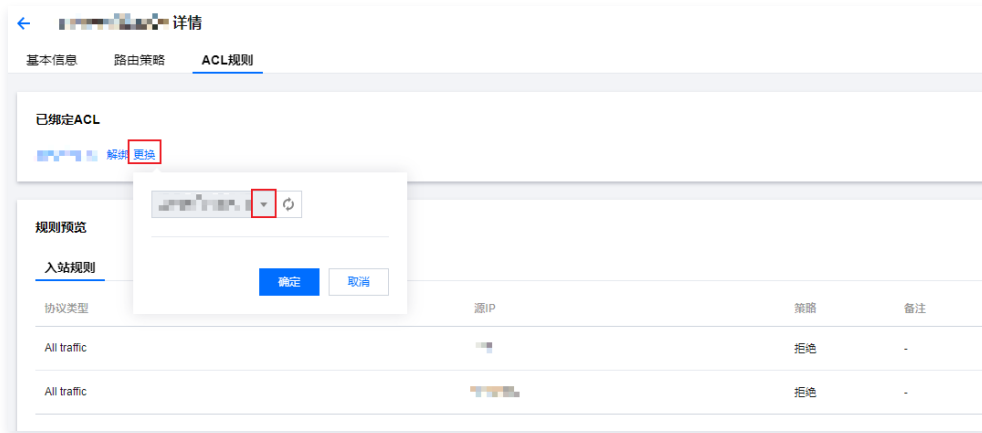


4. 请根据业务需要执行如下操作（此处截图以 ACL 页签操作为例）：

- 如果当前子网未绑定 ACL 规则，可单击**绑定**，选择合适的 ACL 规则，并单击**确定**完成绑定，绑定后立即生效，此时子网的出入流量只有规则策略为**允许**的流量才能通过。



- 如果当前子网绑定的 ACL 规则不符合业务需要，您可以单击**更换**，更换 ACL 规则，更换后立即生效。



- 如果当前子网绑定了 ACL 规则，但您已不再需要控制子网的出入流量，可以单击**解绑**进行 ACL 规则的解绑。解绑成功后立即生效，此时子网的出入流量无规则限制。



# 开启或关闭广播

最近更新时间：2024-04-19 16:50:01

## 背景信息

组播和广播是一对多的通信方式，通过单点到多点的高效数据传送，可以为企业节约网络带宽、降低网络负载。

如果使用单播技术，发送主机需要分别向 N 个主机发送，共发送 N 次；如果使用组播和广播，主机向 N 个主机发送相同的数据时，只要发送1次，既节省服务器资源，也节省了网络主干的带宽资源。

- 组播：腾讯云支持私有网络维度的组播。
- 广播：腾讯云支持子网维度的广播。

### 说明

- 内测申请已结束，公测敬请期待！
- 目前支持组播和广播的地域为：北京、上海、广州、成都、重庆、南京、中国香港、新加坡、首尔、东京、曼谷、多伦多、硅谷、弗吉尼亚、法兰克福、深圳金融、上海金融、北京金融。
- 单 VPC 组播、广播最大支持5万 pps、190Mbps。

## 操作场景

组播和广播较多应用于金融和游戏行业：

- 金融行业主要用于广播业务或行情数据。例如，获取股票价格等实时数据时，券商可通过广播，对多台 client 实时发送股票数据，有效降低网络负载。
- 游戏行业主要用于多台服务器之间的心跳保持。

本章节介绍子网维度的广播功能的开启与关闭。

## 操作步骤

### 开启广播

1. 登录 [私有网络控制台](#)。
2. 在左侧目录中单击子网，进入管理页面。
3. 在列表中，找到需要开启广播功能的子网所在行，单击子网广播下的开启并确认操作即可。



### 关闭广播

1. 登录 [私有网络控制台](#)。
2. 在左侧目录中单击子网，进入管理页面。
3. 在列表中，找到需要关闭广播功能的子网所在行，单击子网广播下的关闭图标并确认操作即可。

## 相关操作

私有网络维度的组播功能的操作指导请参考 [开启或关闭组播功能](#)。

## 删除子网

最近更新时间：2023-10-27 14:27:32

对于子网不再使用，且子网中没有占用 IP 资源时，可进行删除操作。

### 说明

目前子网中涉及 IP 占用的云资源包括：云服务器、内网负载均衡、弹性网卡、HAVIP、云函数 SCF、容器服务、云数据库（例如 MySQL、Redis、TDSQL）等。

## 操作步骤

1. 登录 [私有网络控制台](#)。
2. 在左侧目录中单击子网，进入管理页面。
3. 在列表上方，选择需要删除的子网所在地域和私有网络。
4. 在列表中，找到需要删除的子网所在行，单击操作列的删除，并单击确定即可。



The screenshot shows the Tencent Cloud Private Network console interface. At the top, there are filters for '子网' (Subnet) in '广州' (Guangzhou) and '全部私有网络' (All Private Networks). Below the filters, there is a search bar and a table of subnets. The table has columns for ID/Name, Belonging Network, CIDR, IPv6 CIDR, Available Region, Associated Route Tables, Cloud Servers, Available IP, Default Subnet, Creation Time, and Operations. One row is visible with a '删除' (Delete) button highlighted in red in the Operations column.

ID/名称	所属网络	CIDR	IPv6 CIDR	可用区	关联路由表	云服务器	可用IP	默认子网	创建时间	操作
su De	Vf Di	1; /20	-	广州六区	ri di	5	4086	是	2020-11-12 16:20:16	删除 更多

# 路由表

## 概述

最近更新时间：2023-12-18 16:55:32

路由表由多条路由策略组成，用于控制私有网络内子网的出流量走向。每个子网只能关联一个路由表，一个路由表可以关联多个子网。您可以创建多个路由表，为不同流量走向的子网关联不同的路由表。您可通过如下视频了解路由表的相关信息。

[观看视频](#)

## 类型

路由表有默认路由表和自定义路由表两种类型：

- 默认路由表**：用户创建私有网络时，系统会自动为其生成一个默认路由表。在之后的子网创建过程中，如果用户没有选择自定义路由表，子网会自动关联该默认路由表。您可以在默认路由表中添加、删除和修改路由策略，但无法删除该默认路由表。
- 自定义路由表**：您可以在私有网络中创建自定义路由表，自定义路由表可以被删除，删除前需要解除所有和子网的关联。您可以为具有相同路由策略的子网建立一个自定义路由表，并将路由表与需要遵循其路由策略的所有子网关联。

ID/名称	类型	所属网络	关联子网数	创建时间	标签	操作
rtb-6x3zw0mr test	自定义表	vpc-0ff7ayly lester-test	0	2023-07-17 20:29:31		删除 更多
rtb-ij91zvf default	默认路由表	vpc-0ff7ayly lester-test	1	2023-07-14 11:32:54		删除 更多

### 说明

您可以在 [创建子网](#) 时关联路由表，或在子网创建后，[更换子网关联路由表](#)。

## 路由策略

路由表通过路由策略来实现流量走向控制，路由策略由目的端、下一跳类型和下一跳组成：

- 目的端**：目的端即为您要转发到的目标网段。目的网段描述仅支持网段格式，如果您希望目的端为单个 IP，可设置掩码为 32（如 172.16.1.1/32）。另外，目的端不能为路由表所在私有网络内的 IP 段，原因是 Local 路由已表示此私有网络内默认内网互通。

### 说明

- 如果您的 VPC 中部署了 [容器服务](#)，在新增配置 VPC 子网路由表策略时，目的端网段不能在 VPC 网段范围内，也不能在 [容器网段](#) 范围内。
- 如容器网络和 VPC 已有路由重叠时，则优先在容器网络内转发。

- 下一跳类型**：私有网络的数据包的出口。私有网络下一跳类型支持“NAT 网关”、“对等连接”、“VPN 网关”、“专线网关”、“云服务器”等类型。
- 下一跳**：指定具体跳转到的下一跳实例（使用下一跳 ID 标识），如私有网络内的某个具体 NAT 网关。

## 路由策略优先级

当路由表中存在多条路由策略时，路由优先级由高至低分别为：

- 私有网络内流量**：私有网络内流量最优先匹配。
- 最精确路由（最长前缀匹配）**：当路由表中有多条条目可以匹配目的 IP 时，采用掩码最长（最精确）的一条路由作为匹配项并确定下一跳。
- 公网 IP**：路由策略均匹配失效时，通过公网 IP 对 Internet 进行外访。

### 场景举例：

当一个子网关联了 NAT 网关，且子网内云服务器有公网 IP（或弹性公网 IP）时，会默认通过 NAT 网关访问 Internet（因为最精确路由的优先级高于公网 IP），但您可以设置路由策略，实现通过云服务器公网 IP 访问 Internet，详情请参见 [调整 NAT 网关和 EIP 的优先级](#)。

## 等价路由

等价路由 ECMP（Equal-Cost Multipath Routing），是指到达同一目的地址存在多条相同代价的不同路径。在数据包传输时，如果使用传统的路由技术，去往同一目的地址的数据包仅能利用其中一条路径，而其他路径处于备份或者无效状态，当一条路径故障时，切换路径也需要耗费一定的时间，而等价路由可以在网络环境下同时使用多条路径，不仅增加了传输带宽，也实现了多路径流量负载均衡和冗余链路备份的目的。

- VPC 同类型路由形成 ECMP 的情况如下：



下一跳类型	是否支持同类型形成 ECMP	ECMP 支持的最大数量
NAT 网关	是	N/A
云服务器公网 IP	否	N/A
云服务器	是	同类型最多8个
对等连接	否	N/A
专线网关	否	N/A
云联网	否	N/A
高可用虚拟 IP	是	同类型最多8个
VPN 网关	是	同类型最多8个
云联网（自定义路由）	否	N/A

• VPC 不同类型路由形成 ECMP 的情况如下：

- NAT 网关和云服务器可形成 ECMP。
- 如已有自学习的云联网路由，当新增配置到专线网关/对等连接的自定义路由时，云联网与专线网关/对等连接可形成 ECMP。
- 如已有专线网关/对等连接的自定义路由，当加入云联网，且希望和云联网形成 ECMP 时，请联系 [在线咨询](#)。

## 应用场景

等价路由通常用于：当网关承载带宽有限时，可通过路由实现网关间的流量负载。例如某用户在云上 VPC 和云下 IDC 业务通信带宽需要2000Mbps，但目前 VPN 带宽最大为1000Mbps，那么可以创建两个1000Mbps规格的 VPN 网关，建立两条 VPN 隧道来实现流量分担，两条 VPN 链路可以满足总带宽达到2000Mbps 的需求。

## 主备路由

主备路由是指去往同一目的地址配置了2条或多条路径，而只有1条路径处于活跃状态，其他路径则处于备用或无效状态。例如 VPC 去往某 IDC 配置了两条路由，即路径 A 和路径 B，数据包仅通过主路径 A 去往目的地址，路径 B 处于无效备用状态；当路径 A 发生链路故障时，可使能路径 B 生效，流量则从路径 A 切换到路径 B，保证了业务的可用性，这种情况下称路径 A、B 为主备路由。

VPC 路由表在添加路由策略时，根据下一跳类型定义了不同的优先级，即去往同一目的端，可以配置下一跳为不同类型的网关，形成主备路由，再结合 VPC 网络探测功能，探测链路质量和可达性，通过配置告警及时发现链路异常，快速切换主备路由，以满足业务高可用。

### 说明

- VPC 默认没有路由优先级功能，该功能目前处于内测中，如需使用，请联系 [在线咨询](#)。
- VPC 路由表中根据不同的下一跳类型定义了不同的优先级，目前默认路由优先级为：云联网 > 专线网关 > VPN 网关 > 其他。
- 暂不支持控制台修改优先级，如需调整，请联系 [在线咨询](#)。

VPC 不同类型路由支持主备情况如下：

下一跳类型	是否支持主备
NAT 网关	否
云服务器公网 IP	否
云服务器	是，支持与云联网/VPN 网关/专线网关/高可用虚拟 IP 形成主备
对等连接（同地域）	否
对等连接（跨地域）	否
专线网关	是，支持与云联网/VPN 网关/高可用虚拟 IP/云服务器形成主备
云联网	是，支持与 VPN/专线网关/高可用虚拟 IP/云服务器形成主备
高可用虚拟 IP	是，支持与云联网/VPN 网关/专线网关/云服务器形成主备
VPN 网关	是，支持与云联网/专线网关/高可用虚拟 IP/云服务器形成主备

云联网（自定义路由）

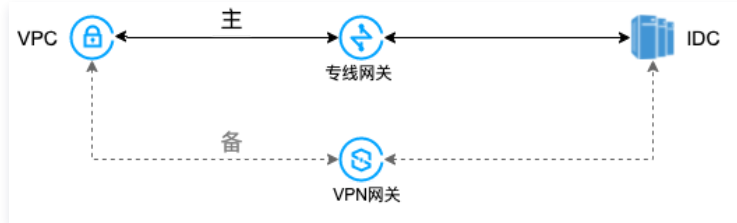
是，支持与 VPN/专线网关/高可用虚拟 IP/云服务器形成主备

### 应用场景

主备路由通常用于：当某一网关链路故障时，可通过主备路由实现流量的平滑切换。例如：

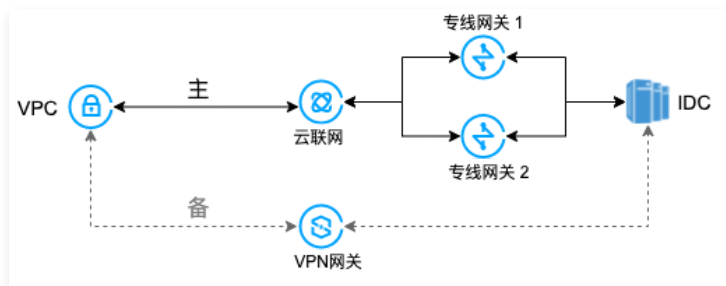
- VPC 型专线网关（主）& VPC 型 VPN 网关（备）

**场景描述：**用户通过 VPC 型专线网关打通云上 VPC 和自建 IDC 的通信，同时通过 VPN 网关创建 VPN 备用通道来实现 IDC 与 VPC 通信链路的备份。



- 云联网型专线网关（主）& VPC 型 VPN 网关（备）

**场景描述：**用户通过云联网型专线网关打通云上 VPC 和自建 IDC 的通信，同时通过 VPN 网关创建 VPN 备用通道来实现 IDC 与 VPC 通信链路的备份。



## 限制说明

最近更新时间：2024-04-11 17:48:41

- 每个私有网络的默认路由表无法删除。
- 创建私有网络后，系统会在路由表中自动添加一条默认路由，表示此私有网络内所有资源均内网互通，该路由策略无法修改和删除。

目的端	下一跳类型	下一跳
Local	Local	Local

- 不支持 BGP 和 OSPF 等动态路由协议。
- 云联网络路由与自定义路由策略重叠时，默认从云联网学习到的路由不生效。若自定义路由支持 ECMP，则可以手动开启云联网络路由，若自定义路由不支持 ECMP，则云联网络路由无法启用。
- 云联网络路由发布策略说明，目前仅支持如下路由类型发布到云联网：

下一跳类型	是否默认发布到云联网	是否支持手工发布/撤回	说明
Local	是	否	VPC 系统路由，接入云联网的 VPC 网段自动发布到云联网，包括主 CIDR 和辅助 CIDR（非容器网段）。
云服务器	否	是	自定义到云服务器的路由策略，其中全0网段路由或者路由策略被禁用时，禁止发布到云联网。
高可用虚拟 IP	否	是	自定义到高可用虚拟 IP 的路由策略，其中全0网段路由或者路由策略被禁用时，禁止发布到云联网。
私网 NAT 网关	否	是	自定义到私网 NAT 网关的路由策略，路由策略被禁用时，禁止发布到云联网。
公网 NAT 网关	否	是	自定义到公网 NAT 网关的路由策略，路由策略被禁用时，禁止发布到云联网，同时仅标准型 NAT 网关

### 说明

- 自定义路由被禁用时，不允许发布到云联网。
- 自定义路由已发布到云联网时，不允许禁用，如果需要，请先撤回，详情可参见 [发布/撤销路由策略到云联网](#)。
- 高可用虚拟 IP 未绑定云服务器时，无法发布到云联网，请绑定后重试。

## 配额限制

资源	限制（单位：个）
每个私有网络内的路由表个数	10
每个子网关联路由表个数	1
每个路由表的路由策略数	50

# 创建自定义路由表

最近更新时间：2024-04-11 09:59:31

路由表用于控制子网出流量的走向，包含多条路由策略。路由表有系统自动生成的默认路由表和用户自定义的路由表。默认路由表（Local 路由）由系统下发，表示 VPC 内网互通，不能被删除，但可以在默认路由表中配置路由策略，配置方法与自定义路由表相同。本章节主要介绍用户自定义路由表的创建和配置。您可以通过如下视频了解如何配置路由表。

[观看视频](#)

## 操作步骤

1. 登录 [私有网络控制台](#)。
2. 单击左侧目录中的路由表，进入管理页面。
3. 单击新建。
4. 在对话框中，输入路由表名称、选择所属私有网络、配置路由策略。

新建路由表
✕

名称   
您还可以输入60个字符

所属网络 vpc-12345678901234567890

标签 标签键 标签值 ✕  
[+ 添加](#)

**路由策略**

📘 路由策略用于控制子网内的流量走向，操作帮助请参考[配置路由策略](#)。

目的端	下一跳类型	下一跳	备注	操作
Local	LOCAL	Local	系统默认下发，表示 VPC 内云服务...	-
<input style="width: 100px;" type="text" value="如 10.0.0.0/16"/>	<span>云服务器的公网IP</span>	云服务器的公网IP <span>📘</span>	<input style="width: 100px;" type="text"/>	<span>✕</span>

[+ 新增一行](#)

创建
关闭

### 📘 说明

路由策略可以在创建路由表时配置，也可以在创建路由表之后，单击路由表 ID 进入详情页面，单击[新增路由策略](#)配置，配置方法相同。

### 配置路由策略：

配置参数	参数说明
目的端	<p>目的端即为您要转发到的目标网段，配置要求如下：</p> <ul style="list-style-type: none"> <li>目的网段描述仅支持网段格式，如果您希望目的端为单个 IP，可设置掩码为32（例如172.16.1.1/32）。</li> <li>目的端不能为路由表所在私有网络内的 IP 段，原因是 Local 路由已表示此私有网络内默认内网互通。</li> </ul> <div style="border: 1px solid #00aaff; padding: 5px; margin-top: 10px;"> <p><b>📘 说明：</b> 当您在 VPC 中部署了 <a href="#">容器服务</a>，在配置 VPC 子网路由表策略时，目的端不能在 VPC 的 CIDR 范围内，也不能包含容器网段。例如某 VPC CIDR 为 `172.168.0.0/16`，容器网络 CIDR 为 `192.168.0.0/16`，那么配置 VPC 子网路由表策略时，目的端网段不能在 `172.168.0.0/16` 范围内，也不能包含 `192.168.0.0/16`。</p> </div>
下一跳类型	私有网络数据包的出口，支持如下类型：

	<ul style="list-style-type: none"> <li>公网 NAT 网关：将指向目标网段的流量转发到一个公网 NAT 网关。</li> <li>私网 NAT 网关：将指向目标网段的流量转发到一个私网 NAT 网关。</li> <li>对等连接：将指向目标网段的流量转发到对等连接另一端的 VPC。</li> <li>专线网关：将指向目标网段的流量转发到一个专线网关。</li> <li>高可用虚拟 IP：将指向目标网段的流量转发到一个高可用虚拟 IP。</li> <li>VPN 网关：将指向目标网段的流量转发到一个 VPN 网关。</li> <li>云服务器的公网 IP：将指向目标网段的流量转发到私有网络内的一台 CVM 实例的公网 IP（包括普通公网 IP 和弹性 IP）。</li> <li>云服务器：将指向目标网段的流量转发到私有网络内的一台 CVM 实例。</li> <li>CDC 本地网关：本地专用集群 CDC 通过 CDC 本地网关与用户 IDC 通信。</li> <li>云联网（自定义路由）：将指向目标网段的流量转发到一个云联网实例。</li> </ul>
下一跳	指定具体跳转到的下一跳实例，如网关或云服务器 IP 等。
备注	可自行添加路由条目的描述信息，便于资源管理。
新增一行	如需配置多条路由策略，可单击新增一行，如需删除可单击操作列的删除图标，创建自定义路由表时，至少需要配置一条路由策略。

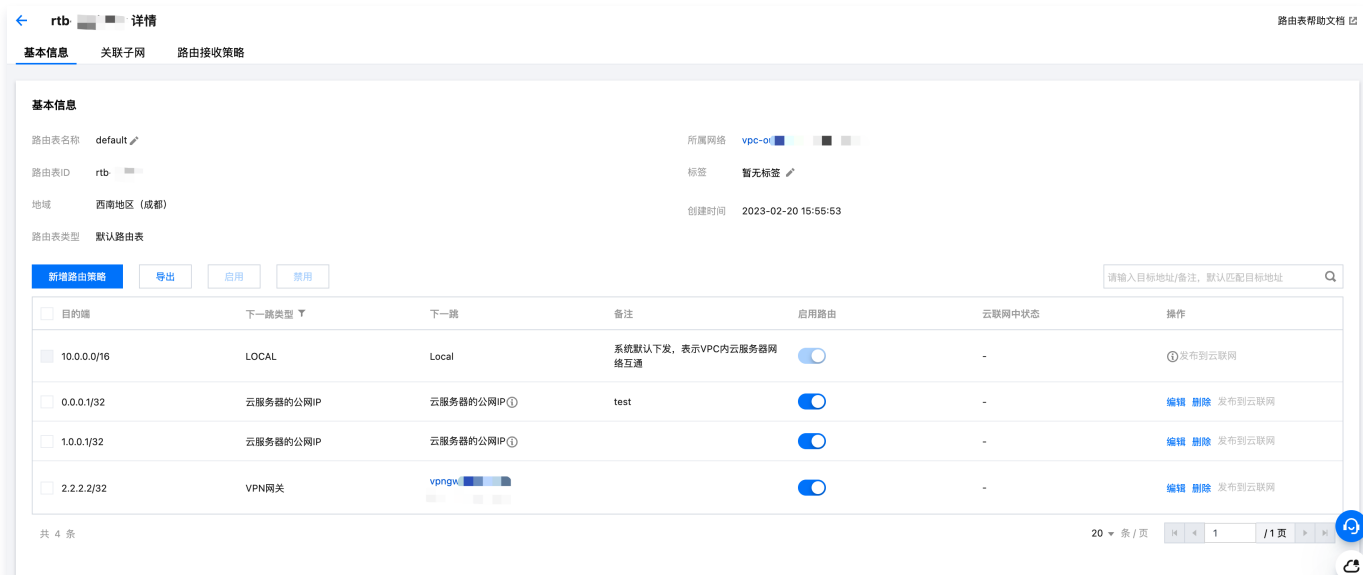
5. 完成参数配置后，单击**创建**即可完成路由表及策略的配置。创建成功的路由表展示在列表中。



## 后续操作

如果您的路由表（包括默认路由表和自定义路由表）中有**下一跳类型**为**高可用虚拟 IP**或**云服务器**的路由策略，则腾讯云支持手动发布或撤销到云联网。

1. 单击路由表 ID 进入路由表详情页面。



2. 可根据实际需求执行如下操作：

- 当路由策略状态为启用，且该VPC已经关联云联网时，单击**发布到云联网**，可手动将该条路由策略发布到云联网。
- 对于已发布到云联网的自定义路由，可单击**从云联网撤回回收策略**。
- 单击**编辑**可修改该条路由策略。
- 策略状态为禁用时，可单击**删除**，删除路由策略。

# 关联与解关联子网

最近更新时间：2024-03-19 10:30:42

路由表创建后，需要关联到子网，才能控制子网的出方向流量。本章节介绍路由表如何与子网关联和解关联。

## 关联子网

1. 登录 [私有网络控制台](#)。
2. 单击左侧目录中的路由表，进入管理页面。
3. 关联子网可通过如下两种方式：
  - 在列表中，找到需要关联子网的路由表，单击操作列的**关联子网**。



- 单击路由表 ID 进入详情页下的**关联子网**网页签，单击**新增关联子网**。



4. 在弹出框中，选择待关联的子网（一个路由表可同时选择多个子网关联，支持通过子网 ID/名称快速筛选），请评估关联后对子网的业务影响，确认无误后，单击**确定**。

### 注意

路由表关联到子网后，子网原先关联的路由表将被替换为该路由表，子网出流量策略将按该路由表中的策略执行，请仔细评估业务影响。



### 解关联子网

1. 登录 [私有网络控制台](#)。
2. 单击左侧目录中的**路由表**，进入管理页面。
3. 单击路由表 ID 进入详情页下的**关联子网**网页签，单击**解关联**。



4. 在弹出框中，为解关联的子网重新选择一个路由表，并单击**确定**即可完成子网对当前路由表的解关联操作，同时子网出向流量策略将按照最新为其选择的**路由表**处理。

### 解关联子网 ✕

搜索名称或ID 🔍

id/名称	现关联
<input type="radio"/> rtb- [模糊]	现关联
<input checked="" type="radio"/> rtb- [模糊]	

⚠️ 解关联子网后，该子网需要重新关联一个路由表，请选择路由表

确定 关闭



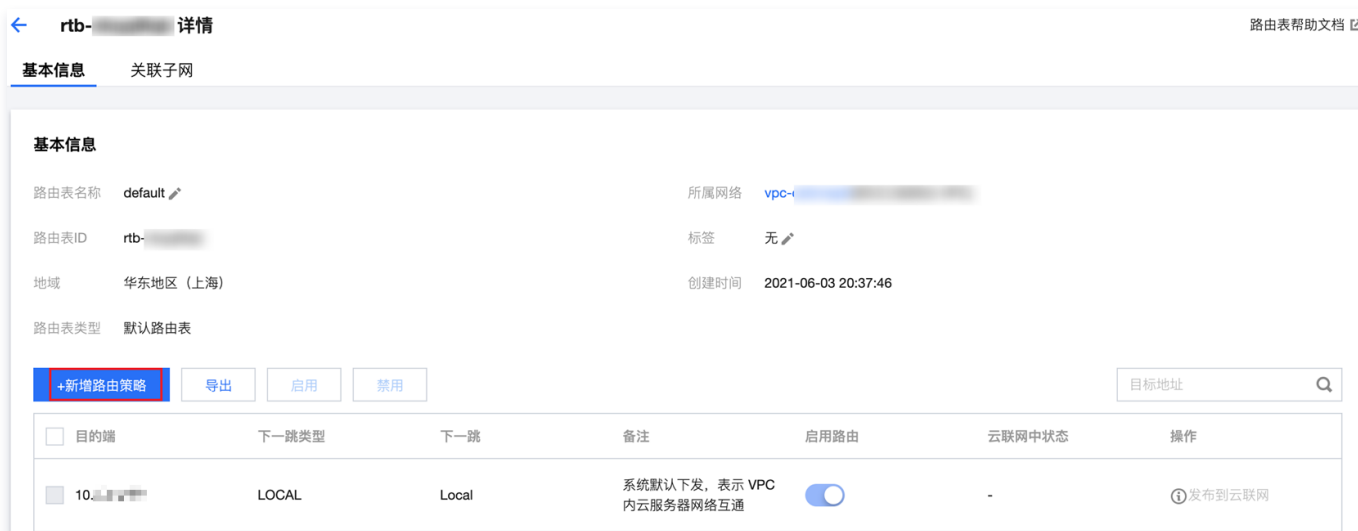
# 管理路由策略

最近更新时间：2024-04-11 09:59:31

路由表中的路由策略支持实时增删、查询与导出、手动发布或撤销云联网、启用或禁用等配置操作，本章节主要介绍路由策略的相关操作指导。

## 新增路由策略

1. 登录 [路由表控制台](#)，进入路由表管理界面。
2. 在列表中，单击需要修改的路由表 ID，进入详情页。
3. 单击新增路由策略。



4. 在弹出框中，配置路由策略。

### 说明

当您在 VPC 中部署了 [容器服务](#)，在配置 VPC 子网路由表策略时，目的端不能在 VPC 的 CIDR 范围内，也不能包含容器网段。例如某 VPC CIDR 为 172.168.0.0/16，容器网络 CIDR 为 192.168.0.0/16，那么配置 VPC 子网路由表策略时，目的端网段不能在 172.168.0.0/16 范围内，也不能包含 192.168.0.0/16。

配置	说明
目的端	子网出流量要转发到的目标网段，要求如下： <ul style="list-style-type: none"> <li>目的网段描述仅支持网段格式，如果您希望目的端为单个 IP，可设置掩码为 32（例如 172.16.1.1/32）。</li> <li>目的端不能为路由表所在私有网络内的 IP 段，原因是 Local 路由已表示此私有网络内默认内网互通。</li> </ul>
下一跳类型	私有网络数据包的出口，支持如下类型： <ul style="list-style-type: none"> <li>NAT 网关：将指向目标网段的流量转发到一个 NAT 网关。</li> <li>对等连接：将指向目标网段的流量转发到对等连接另一端的 VPC。</li> <li>专线网关：将指向目标网段的流量转发到一个专线网关。</li> <li>高可用虚拟 IP：将指向目标网段的流量转发到一个高可用虚拟 IP。</li> <li>VPN 网关：将指向目标网段的流量转发到一个 VPN 网关。</li> <li>云服务器的公网 IP：将指向目标网段的流量转发到私有网络内的一台 CVM 实例的公网 IP（包括普通公网 IP 和弹性 IP）。</li> <li>云服务器：将指向目标网段的流量转发到私有网络内的一台 CVM 实例。</li> <li>CDC 本地网关：本地专用集群 CDC 通过 CDC 本地网关与用户 IDC 通信。</li> <li>云联网（自定义路由）：将指向目标网段的流量转发到一个云联网实例。</li> </ul>
下一跳	指定具体跳转到的下一跳实例，如网关或云服务器 IP 等。
备注	可自行添加路由条目的描述信息，便于资源管理。
新增一行	如需配置多条路由策略，可单击新增一行，如需删除可单击操作列的删除图标。

**新增路由** ×

① 路由策略用于控制子网内的流量走向，操作帮助请参考[配置路由策略](#)。

目的端	下一跳类型	下一跳	备注	操作
<input type="text" value="如 10.0.0.0/16"/>	<input type="text" value="云服务器的公网IP"/>	<input type="text" value="云服务器的公网IP ①"/>	<input type="text"/>	<input type="button" value="✕"/>

[+新增一行](#)

5. 单击**创建**，完成路由策略的配置。

### 编辑路由策略

1. 登录 [路由表控制台](#)，进入路由表管理界面。
2. 在列表中，单击路由表 ID，进入详情页。
3. 单击路由策略右侧的**编辑**，可对该条路由由条目进行修改。

目的端	下一跳类型	下一跳	备注	启用路由	云联网中状态	操作
10.0.0.0/16	LOCAL	Local	系统默认下发，表示 VPC 内云服务器网络互通	<input checked="" type="checkbox"/>	已发布	<a href="#">① 从云联网撤回</a>
172.16.0.0/16	LOCAL	Local	系统默认下发，表示 VPC 内云服务器网络互通	<input checked="" type="checkbox"/>	-	<a href="#">① 发布到云联网</a>
10.0.0.0/16	云联网	cc1		<input checked="" type="checkbox"/>	-	<a href="#">① 发布到云联网</a>
10.0.0.0/16	云联网	ccn		<input checked="" type="checkbox"/>	-	<a href="#">① 发布到云联网</a>
81.0.0.0/16	云服务器的公网IP	云服务器的公网IP ①	go	<input checked="" type="checkbox"/>	-	<a href="#">编辑</a> <a href="#">删除</a> <a href="#">发布到云联网</a>

4. 修改完成后，单击**确定**即可，单击**取消**可取消该操作。

### 发布/撤销路由策略到云联网

通常关联到云联网的 VPC，默认路由已经发布到云联网。针对未默认发布进云联网的新增自定义路由策略，需要手动发布进云联网，也支持从云联网撤回。而默认已经发布进云联网的路由策略，也支持从云联网撤回。

当前支持路由表中下一跳类型为**高可用虚拟 IP**、**云服务器**、**私网 NAT 网关**和**标准型公网 NAT 网关**的自定义路由策略手动发布或撤销到云联网。

### 前提条件

高可用虚拟 IP、云服务器、私网 NAT 网关和标准型公网 NAT 网关所在的私有网络已关联至云联网。

### 操作步骤

1. 登录 [路由表控制台](#)，进入路由表管理界面。
2. 在列表中，单击需要修改的路由表 ID，进入详情页。
3. 可根据实际需求执行如下操作：
  - 对于自定义路由策略，可单击**发布到云联网**，可手动将该条路由策略发布到云联网。
  - 对于已发布到云联网的自定义路由策略，可单击**从云联网撤回**回收策略。

**注意**

- 当路由策略的状态为禁用时，不允许发布进云联网。
- 当路由策略已发布进云联网时，不允许禁用路由策略。

### 查询与导出路由策略

1. 登录 [路由表控制台](#)，进入路由表管理界面。

2. 在列表中，单击路由表 ID，进入详情页，可查看到当前路由表中包含的路由策略。
3. 在右上方搜索框中，支持通过目标地址快速查询。



4. 单击导出，可导出当前界面显示的路由策略，以.csv 格式保存。

## 启用/禁用路由策略

您可以对自定义路由策略执行启用/禁用操作。

### 操作步骤

1. 登录 [路由表控制台](#)。
2. 单击路由表 ID 进入详情界面，路由策略状态如下：
  - 表示路由策略处于启用状态
  - 表示路由策略处于禁用状态
3. 禁用路由策略：单击某条处于启用状态的路由策略右侧的图标 ，可禁用该条路由策略。

#### 注意

路由条目禁用可能导致业务中断，请谨慎评估后再操作。



4. 启用路由策略：单击某条处于禁用状态的路由策略右侧的图标 ，可启用该条路由策略。

#### 注意

路由条目启用后，将按照最长掩码匹配选路，可能会影响当前业务转发，请仔细评估后再操作。

### 确定启用该路由策略？

确认启用后，将按最长掩码匹配选路。

确认 取消

5. 批量启用或禁用路由：如需对多条路由策略批量执行启用或禁用操作，可勾选具体路由条目，然后单击上方的启用或禁用进行批量操作，例如下图中批量禁用多条路由条目。

目的端	下一跳类型	下一跳	备注	启用路由	云联网中状态	操作
<input checked="" type="checkbox"/> 32	云联网	ccn-2ouaeabl		<input checked="" type="checkbox"/>	-	发布到云联网
<input checked="" type="checkbox"/> 32	云联网	ccn-2ouaeabl		<input checked="" type="checkbox"/>	-	发布到云联网
<input checked="" type="checkbox"/> 16	云联网	ccn-2ouaeabl		<input checked="" type="checkbox"/>	-	发布到云联网

### 删除路由策略

如您不需要某条路由策略时，可将其删除。只有自定义路由策略支持删除。

1. 登录 [路由表控制台](#)，进入路由表管理界面。
2. 在列表中，单击需要修改的路由表 ID，进入详情页。
3. 单击需要删除的路由策略条目右侧的删除。

目的端	下一跳类型	下一跳	备注	启用路由	云联网中状态	操作
10.0.0.0/24	LOCAL	Local	系统默认下发，表示 VPC 内云服务器网络互通	<input checked="" type="checkbox"/>	已发布	从云联网撤回
172.16.0.0/16	LOCAL	Local	系统默认下发，表示 VPC 内云服务器网络互通	<input checked="" type="checkbox"/>	-	发布到云联网
10.0.0.0/24	云联网	ccn-xxxxxx		<input checked="" type="checkbox"/>	-	发布到云联网
10.0.0.0/24	云联网	ccn-xxxxxx		<input checked="" type="checkbox"/>	-	发布到云联网
81.0.0.0/24	云服务器的公网IP	云服务器的公网IP	90.0.0.0/24	<input checked="" type="checkbox"/>	-	编辑 删除 发布到云联网

4. 请评估策略删除可能存在的业务影响，确认无误后，单击确定即可。

×

**您确认要删除该路由条目吗?**

⚠ 路由条目删除可能导致业务中断，请再次确认变更后的影响

目的端	下一跳类型	下一跳	备注	状态
81.71.140.9...	云服务器的...	云服务器的公 网IP ⓘ	goohenry	已启用

确定取消

# 删除路由表

最近更新时间：2023-10-27 14:27:33

## 前提条件

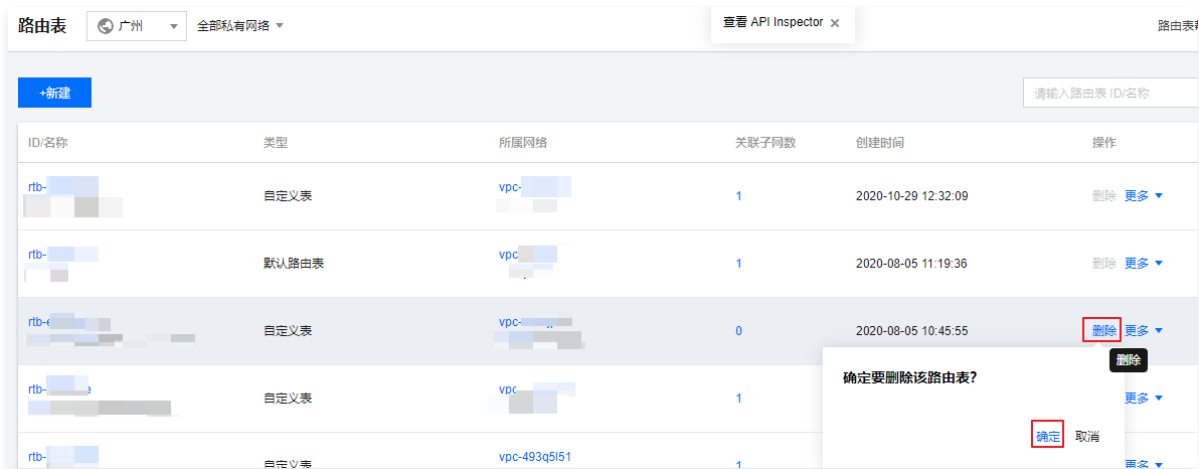
当路由表未关联到任何子网时，可执行删除操作。系统自动生成的默认路由表无法删除，仅支持自定义路由表删除。

### 注意

删除路由表可能导致业务中断，请谨慎操作。

## 操作步骤

1. 登录 [路由表控制台](#)。
2. 在列表中，找到需要删除的路由表所在行，单击操作栏中删除并确认操作即可。



The screenshot shows the Tencent Cloud console interface for route tables. At the top, there are filters for '广州' (Guangzhou) and '全部私有网络' (All Private Networks). A search bar is present with the placeholder text '请输入路由表 ID/名称'. Below the search bar is a table with the following columns: ID/名称, 类型 (Type), 所属网络 (Associated Network), 关联子网数 (Associated Subnets), 创建时间 (Creation Time), and 操作 (Actions). The table contains five entries. The third entry, a custom route table with 0 associated subnets, has a '删除' (Delete) button highlighted with a red box. A modal dialog box is open over this row, asking '确定要删除该路由表?' (Are you sure you want to delete this route table?). The dialog has '删除' (Delete) and '确定' (Confirm) buttons, with '确定' also highlighted with a red box.

ID/名称	类型	所属网络	关联子网数	创建时间	操作
rtb-...	自定义表	vpc-...	1	2020-10-29 12:32:09	删除 更多
rtb-...	默认路由表	vpc-...	1	2020-08-05 11:19:36	删除 更多
rtb-...	自定义表	vpc-...	0	2020-08-05 10:45:55	删除 更多
rtb-...	自定义表	vpc-...	1		删除 更多
rtb-...	自定义表	vpc-493q5151	1		删除 更多

# IP 与网卡

## 弹性公网 IP

最近更新时间：2022-06-16 18:26:46

**弹性公网 IP (EIP)**，简称弹性 IP 地址或弹性 IP。它是专为动态云计算设计的静态 IP 地址，是某地域下一个固定不变的公网 IP 地址。借助弹性公网 IP，您可以快速将地址重新映射到账户中的另一个 CVM 实例或 NAT 网关实例，从而屏蔽实例故障。

弹性公网 IP 未进行释放前，您可以将其一直保留于您的账号中。相较于公网 IP 仅可跟随云服务器一起申请释放，弹性公网 IP 可以与云服务器的生命周期解耦，作为云资源单独进行操作。例如，若您需要保留某个与业务强相关的公网 IP，可以将其转为弹性公网 IP 保留在您的账号中。

关于弹性公网 IP 的常用操作，请参见：

- [申请 EIP](#)
- [EIP 绑定云资源](#)
- [快速搭建 IPv4 私有网络](#)

## 弹性公网 IPv6

最近更新时间：2022-07-18 14:35:20

[弹性公网 IPv6](#)，是云服务器 IPv6 的公网网关，提供 IPv6 的公网访问能力。云服务器申请了 IPv6 地址后，默认关闭了公网访问能力，通过弹性公网 IPv6，您可以为每一个云服务器的 IPv6 地址开通或者关闭公网，并设置公网带宽。

关于弹性公网 IPv6 的常用操作，请参见：

- [私有网络分配与释放 IPv6 CIDR](#)
- [子网分配与释放 IPv6 CIDR](#)
- [弹性网卡申请与释放 IPv6 地址](#)
- [管理 IPv6 公网](#)
- [搭建 IPv6 私有网络](#)



# 高可用虚拟 IP

## 概述

最近更新时间：2023-07-24 18:33:42

高可用虚拟 IP（HAVIP）是从 VPC 子网 CIDR 分配的一个内网 IP 地址，通常和高可用软件（如 keepalived 或 Windows Server Failover Cluster）配合使用，应用于搭建高可用主备集群场景。

### 说明

- 目前 HAVIP 产品处于灰度优化中，切换的时延在10s左右，如有需要，请提交 [工单申请](#)。
- 为保证主备集群云服务器的高可用性，强烈建议通过 [置放群组](#) 将不同云服务器分配到不同的宿主机上，更多关于置放群组的信息，请参见 [置放群组](#)。
- 高可用软件需要支持发送 ARP 报文。

## 特点介绍

- 可以在 HAVIP 产品控制台申请 HAVIP 地址，每个 VPC 可以申请多个 HAVIP 地址。
- 需要在云服务器的配置文件中绑定 HAVIP。

## 架构与实现原理

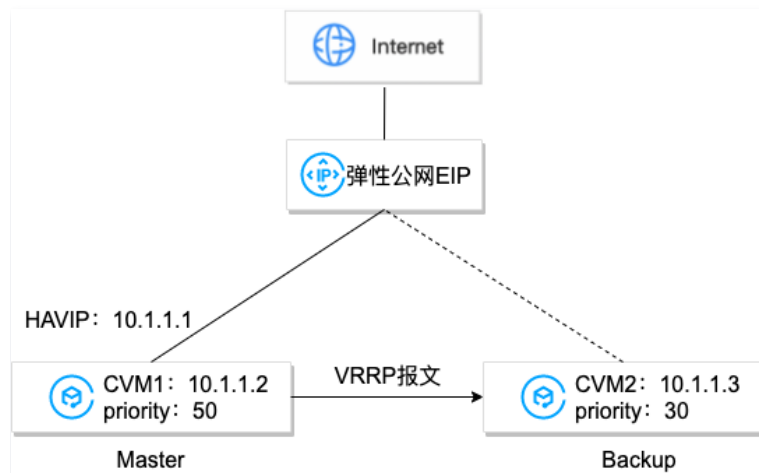
通常高可用主备集群包含2台服务器，一台主服务器处于某种业务的激活状态（即 Active 状态），另一台备服务器处于该业务的备用状态（即 Standby 状态），它们共享同一个 VIP（Virtual IP，一个内网 IP）。同一时刻，VIP 只在一台主设备上生效，当主服务器出现问题时，备用服务器接管 VIP 继续提供服务。

- 在传统物理网络中，可以通过 keepalived 的 VRRP 协议协商主备状态。其原理为：主设备周期性发送免费 ARP 报文刷新上联交换机的 MAC 表或终端 ARP 表，触发 VIP 迁移到主设备上。
- 在私有网络 VPC 中，同样通过在云服务器中部署 keepalived 来实现高可用主备集群。与物理网络不同的是，出于安全考虑（如 ARP 欺骗等），通常不支持云服务器通过 ARP 宣告普通内网 IP，该 VIP 必须为从腾讯云申请的高可用虚拟 IP（HAVIP），且该 VIP 具有子网属性，只能在同一子网下的机器间宣告绑定。

### 说明

keepalived 是基于 VRRP 协议的一款高可用软件，keepalived 配置通过 keepalived.conf 文件完成。

高可用虚拟 IP 的架构如下图所示。



以上图举例，假设搭建 CVM1 和 CVM2 为一套高可用主备集群，实现原理如下：

1. CVM1 和 CVM2 均安装 keepalived 软件，配置 HAVIP 为 VRRP VIP，并设置主备服务器的优先级（priority 值），值越大优先级越高。
2. keepalived 中的 VRRP 协议通过比对 CVM1 和 CVM2 的初始优先级大小，选举出 Master 服务器，即 CVM1 为 Master 服务器，CVM2 为 Backup 服务器。
3. Master 服务器向外发送 ARP 报文，宣告 VIP（该 VIP 为 HAVIP），并更新 VIP 和 MAC 的地址映射。此时，真正对外提供服务的服务器为 Master 服务器，通信的内网 IP 为 HAVIP。同时，可在 HAVIP 控制台看到，HAVIP 绑定的服务器为 Master 服务器 CVM1。
4. （可选）可以在控制台为 HAVIP 绑定 EIP，实现公网交互。
5. Master 服务器会周期性发送 VRRP 报文给 Backup 服务器。如果 Master 服务器异常，Backup 服务器在一定时间内没有收到 VRRP 报文，则会将将自己设置为 Master，并对外发送 ARP 更新，报文携带自己的 MAC 地址，此时 Backup 服务器 CVM2 将作为 Master 服务器对外提供通信服务，外部访问的报文将转发至 CVM2 处理。在 HAVIP 控制台可看到 HAVIP 绑定的云服务器变更为 CVM2。

## 常见使用场景

- 负载均衡的 HA

用户自己部署负载均衡时，一般业务架构是：负载均衡之间做 HA，后端机器做集群。因此部署负载均衡的两台服务器间要部署 HA，用 HAVIP 作为 virtual IP。

- 关系型数据库主备

两台数据库之间通过 keepalived 或 Windows Server Failover Cluster 搭建高可用主备集群，需要 HAVIP 作为 virtual IP。详细操作请参见 [最佳实践-用 HAVIP+Keepalived 搭建高可用主备集群](#) 和 [最佳实践-用 HAVIP + Windows Server Failover Cluster 搭建高可用 DB](#)。

## 常见问题

### 为什么在 VPC 环境，需要使用 HAVIP 配合 keepalived?

公有云厂商的普通内网 IP，出于安全考虑（如 ARP 欺骗等），不支持主机通过 ARP 宣告 IP。如果用户直接在 keepalived.conf 文件中指定一个普通内网 IP 为 virtual IP，当 keepalived 将 virtual IP 从 MASTER 机器切换到 BACKUP 机器时，将无法更新 IP 和 MAC 地址的映射，而需要调 API 来进行 IP 切换。以 keepalived 配置为例，IP 相关部分如下：

```
vrrp_instance VI_1 {
    state BACKUP          #备
    interface eth0        #网卡名
    virtual_router_id 51
    nopreempt             #非抢占模式
    #preempt_delay 10
    priority 80
    advert_int 1
    authentication {
        auth_type PASS
        auth_pass 1111
    }
    unicast_src_ip 172.17.16.7 #本机内网 IP
    unicast_peer {
        172.17.16.13          #对端设备的 IP 地址，例如：10.0.0.1
    }

    virtual_ipaddress {

        172.17.16.3 #高可用虚拟IP，填写控制台申请到的 HAVIP 地址。

    }

    garp_master_delay 1
    garp_master_refresh 5

    track_interface {
        eth0
    }

    track_script {
        checkhaproxy
    }
}
```

若没有 HAVIP，以下这段配置文件不生效。

```
virtual_ipaddress {
    172.17.16.3 #高可用虚拟IP，填写控制台申请到的 HAVIP 地址。
}
```

## 后续操作

- 了解 HAVIP 的使用限制，请参见 [限制说明](#)。
- 了解 HAVIP 的操作指南，请参见 [管理 HAVIP](#)。

## 限制说明

最近更新时间：2024-03-13 17:02:41

### 使用限制

- 由后端云服务器宣告占有该 HAVIP，不支持手动在控制台把 HAVIP 绑定指定机器（体验与传统物理机保持一致）。
- 是否发生迁移由后端 RS 根据配置文件协商决定，不是由 HAVIP 决定。
- 仅支持私有网络，不支持基础网络。
- 心跳检测需要在云服务器中的应用来实现，不是靠 HAVIP 实现，HAVIP 仅作为一个被 ARP 宣告的浮动内网 IP（体验与传统物理机保持一致）。
- 高可用虚拟 IP 未绑定云服务器时，无法发布到云联网，请绑定后重试，详情请参见 [云联网路由发布策略限制](#)。

### 配额限制

资源	限制
每个私有网络的 HAVIP 默认配额数	10个

## 创建高可用虚拟 IP

最近更新时间：2023-07-24 18:33:42

本章节介绍如何在控制台创建高可用虚拟 IP（HAVIP），以及 HAVIP 创建后，在第三方软件中如何进行配置等后续操作。

### 说明

目前 HAVIP 产品处于灰度优化中，如有需要，请提交 [工单申请](#)。

### 操作步骤

1. 登录 [私有网络控制台](#)，在左侧导航栏中，选择 **IP 与网卡** > **高可用虚拟 IP**。
2. 在 HAVIP 管理页面，选择所在地域，单击 **申请**。
3. 在弹出的 **申请高可用虚拟 IP** 对话框中，配置 HAVIP 的参数。
  - **名称**：填写 HAVIP 的名称。
  - **私有网络**：选择待创建 HAVIP 所在的私有网络。
  - **子网**：HAVIP 具有子网属性，请选择所在子网。
  - **IP 地址**：支持自动分配和手动填写。选择自动分配系统将从子网中分配一个 IP 地址；选择手动填写，需填写子网网段范围内的可用 IP 地址，且不能为系统保留 IP。例如，所属子网网段为：10.0.0.0/24，则可填的内网 IP 范围为：10.0.0.2 - 10.0.0.254。

申请高可用虚拟IP

绑定子机需要通过软件宣告，控制台暂时不支持绑定子机的操作

名称

所在地域 广州

私有网络

子网

可用区 -

子网CIDR -

子网可用IP -

可分配 0/11

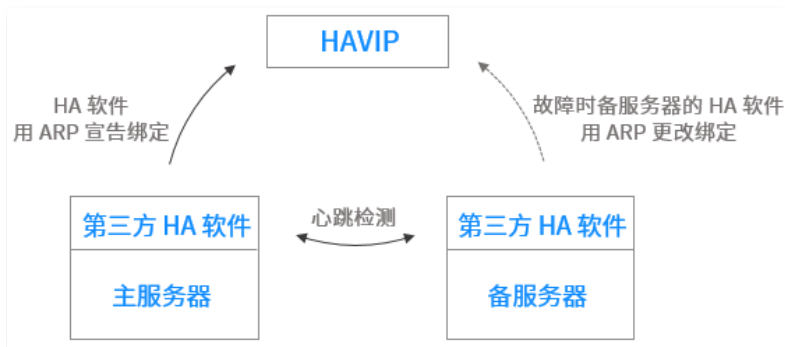
地址  系统将自动分配IP地址

4. 单击 **确定**，创建成功的 HAVIP 展示在列表中，状态为 **未绑定云服务器**。

ID/名称	状态	地址	后端网卡	所属主机	弹性公网IP	所属网络	所属子网	申请时间	操作
havip-xxxx	未绑定云服务器	10.x.x.x	-	-	-	vpc-xxxx	sub-xxxx	2021-05-21 11:3...	<a href="#">绑定弹性IP</a> <a href="#">释放解绑弹性IP</a>

### 后续操作

HAVIP 用于配合第三方 HA 软件使用，创建后还需要在第三方 HA 软件中操作（HAVIP 只是被操作的对象，作为可被声明绑定的内网 IP，操作的发起方为第三方 HA 软件，不在 HAVIP 的控制台实现绑定和解绑）。即：在第三方 HA 软件中，将 HAVIP 指定为可漂移的 VIP（Virtual IP Address），然后由第三方 HA 软件通过 ARP 协议指定 HAVIP 要绑定的网卡。示意图如下：



传统物理设备环境下，所有内网 IP 默认都是可以通过 ARP 协议绑定到网卡上的，都可以在 HA 软件中指定为可漂移的 IP。而在公有云环境下普通内网 IP 禁止 ARP 协议，若在 HA 软件中指定普通内网 IP 为可漂移的 IP，会导致漂移失败，因此在云服务器内的 HA 软件中，需要将 HAVIP 指定为可漂移的 VIP。该操作与第三方 HA 软件在非云平台的操作完全一样。

**说明**

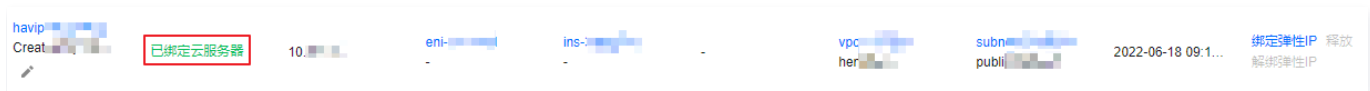
常见的 HA 软件有：Linux 下的 HeartBeat、keepalived、pacemaker，Windows 下的 MSCS 等。

在 HA 软件指定 VIP 时（配置文件），填入您创建的 HAVIP 即可，配置示例如下：

```

vrrp_instance VI_1 {
#注意主备参数选择
state MASTER          #设置初始状态为"备"。
interface eth0        #设置绑定 VIP 的网卡，例如 eth0
virtual_router_id 51  #配置集群 virtual_router_id 值
nopreempt             #设置非抢占模式
preempt_delay 10     #抢占延时10分钟
priority 100         #设置优先级，值越大优先级越高
advert_int 1         #检查间隔，默认1秒
authentication {    #设置认证
  auth_type PASS     #认证方式
  auth_pass 1111     #认证密码
}
unicast_src_ip 172.16.16.5 #设置本机内网IP地址
unicast_peer{
  172.16.16.6        #对端设备的 IP 地址
}
virtual_ipaddress {
  172.16.16.12       #设置“高可用虚拟IP”为可漂移的IP
}
}
    
```

在云服务器的 HA 软件中配置了 HAVIP 后，控制台中该 HAVIP 的状态将变更为**已绑定云服务器**。



常见配置案例请参见：

- [最佳实践 - 用 HAVIP+Keepalived 搭建高可用主备集群](#)
- [最佳实践 - 用 HAVIP+Windows Server Failover Cluster 搭建高可用 DB](#)

**相关文档**

高可用虚拟 IP 与普通内网 IP 类似，均支持在控制台绑定或解绑 EIP，如果您有公网通信的需求，可参考 [绑定或解绑 EIP](#)，如无，可不绑定 EIP。

# 绑定或解绑 EIP

最近更新時間：2023-07-24 18:33:42

高可用虚拟 IP 与普通内网 IP 类似，均支持在控制台绑定或解绑 EIP，如果您有公网通信的需求，可参考本文为其绑定 EIP。如您没有公网通信的需求，可跳过本章节。

## 说明

目前 HAVIP 产品处于灰度优化中，如有需要，请提交 [工单申请](#)。

## 绑定 EIP

1. 登录 [私有网络控制台](#)，在左侧导航栏中，选择 **IP 与网卡 > 高可用虚拟 IP**。
2. 在 HAVIP 管理页面，选择所在地域。
3. 选择待绑定 EIP 的 HAVIP，单击右侧操作列的**绑定**。

ID/名称	状态	地址	后端网卡	所属主机	弹性公网IP	所属网络	所属子网	申请时间	操作
找到 1 条结果 <a href="#">返回原列表</a>									
havip- Creati	已绑定云服务器	172	eni-	ins-		vpc- Defa	sub- Defa	2022-06-18 09:27:16	<a href="#">绑定弹性IP</a> <a href="#">释放弹性IP</a>

4. 在弹出的**绑定弹性公网 IP**对话框中，单击需要绑定的 EIP。

## 注意

- 如无可用的 EIP，请先在 EIP 控制台 [创建 EIP](#) 后再执行绑定操作，一个 HAVIP 只能绑定一个 EIP。
- 如果 HAVIP 未绑定到云服务器实例上，绑定此 HAVIP 的 EIP 将处于**闲置**状态，系统会收取资源闲置费用。因此，请正确配置高可用，确保绑定成功。常见配置案例请参考：
  - [最佳实践 - 用 HAVIP + Keepalived 搭建高可用主备集群](#)
  - [最佳实践 - 用 HAVIP + Windows Server Failover Cluster 搭建高可用 DB](#)

5. 单击**确定**完成 EIP 的绑定。

ID/名称	状态	地址	后端网卡	所属主机	弹性公网IP	所属网络	所属子网	申请时间	操作
找到 1 条结果 <a href="#">返回原列表</a>									
havi- Creati	已绑定云服务器	172	eni-	ins-	11	vpc- Defa	subri- Defa	2022-06-18 09:27:16	<a href="#">绑定弹性IP</a> <a href="#">释放弹性IP</a>
								共 1 条	10 条 / 页 <span>1 / 1 页</span>

## 解绑 EIP

1. 登录 [私有网络控制台](#)，在左侧导航栏中，选择 **IP 与网卡 > 高可用虚拟 IP**。
2. 在 HAVIP 管理页面，选择所在地域。
3. 选择待解绑 EIP 的 HAVIP，单击右侧操作列的**解绑弹性 IP**。
4. 在弹出的**解绑弹性公网 IP**对话框中，请知悉如下风险，确认无误后，单击**确定**完成 EIP 的解绑。

## 注意

- 解绑 EIP 会影响公网业务，请评估业务影响并做好准备。
- 解绑后的 EIP 将处于**闲置**状态，系统会收取资源闲置费用，如不需要，可直接 [释放 EIP](#)。

解绑弹性公网IP ×

确定将该弹性公网IP: 11[redacted]与绑定的HAVIP:havip-[redacted]解绑?  
解绑后, 可能会影响您的业务, 请提前做好准备。

# 查询高可用虚拟 IP

最近更新时间：2023-07-24 18:33:43

在 HAVIP 控制台，可查看指定地域下的所有 HAVIP 详细信息。

## 说明

目前 HAVIP 产品处于灰度优化中，如有需要，请提交 [工单申请](#)。

## 操作步骤

1. 登录 [私有网络控制台](#)。
2. 在左侧导航栏中，选择 [IP 与网卡](#) > [高可用虚拟 IP](#)，进入高可用虚拟 IP 界面。
3. 选择地域，可查看该地域下所有已申请的 HAVIP 的详细信息。

ID/名称	状态	地址	后端网卡	所属主机	弹性公网IP	所属网络	所属子网	申请时间	操作
havip- Cre	已绑定云服务器	10.	en-	ins	-	vpc-	sub-	2022-06-20 03:05:11	绑定弹性IP 释放 解绑弹性IP

字段含义如下：

- **ID/名称**：HAVIP 创建后，系统会自动生成一个 ID，单击 ID 可进入 HAVIP 的基本信息界面；名称为创建时用户自定义的名称。
  - **状态**：表示该 HAVIP 是否已在云服务器的 HA 软件的配置文件中被指定为可漂移的 VIP，如已成功配置，则状态显示为 **已绑定云服务器**，如未配置或配置失败，则状态显示为 **未绑定云服务器**。
  - **地址**：HAVIP 的地址。
  - **后端网卡**：HAVIP 绑定的云服务器的弹性网卡 ID，如 HAVIP 未绑定云服务器，则此处显示为 -。
  - **所属主机**：HAVIP 绑定的云服务器 ID，如 HAVIP 未绑定云服务器，则此处显示为 -。
  - **弹性公网 IP**：HAVIP 绑定的 EIP，如 HAVIP 未绑定 EIP，则此处显示为 -。
  - **所属网络**：HAVIP 所在私有网络。
  - **所属子网**：HAVIP 所在子网。
  - **申请时间**：HAVIP 申请的时间。
  - **操作**：HAVIP 可执行的操作，包括：绑定弹性 IP、解绑弹性 IP、释放。
    - **绑定弹性 IP**：用于绑定 EIP
    - **解绑弹性 IP**：用于解绑 EIP
    - **释放**：用于释放 HAVIP
4. 在右侧搜索框中，可输入 ID、名称或地址，进行快速搜索。
  5. 单击右上角刷新图标，可刷新界面。



# 释放高可用虚拟 IP

最近更新时间：2024-03-13 17:02:41

如果不再使用 HAVIP，可参考本文在控制台将其直接释放。

## 说明：

目前 HAVIP 产品处于灰度优化中，如有需要，请提交 [内测申请](#)。

## 前提条件

仅未绑定云服务器的 HAVIP 支持释放。

## 说明：

对于已绑定云服务器的 HAVIP，如需释放，请先在云服务器的第三方 HA 软件中更改配置文件来解绑 HAVIP 后，才可在控制台执行释放操作。

## 操作步骤

1. 登录 [私有网络控制台](#)。
2. 在左侧导航栏中，选择 IP 与网卡 > 高可用虚拟 IP，在列表中找到需要释放的 HAVIP。
3. 单击操作栏下的释放。

ID/名称	状态	地址	后端网卡	所属主机	弹性公网IP	所属网络	所属子网	申请时间	操作
hvip- [ID]	未绑定云服务器	10.1.1.1	-	-	-	vpc- [ID]	sub- [ID]	2021-05-21 11:39:27	绑定弹性IP 解绑弹性IP 释放
hvip- [ID] Cred- [ID]	已绑定云服务器	10.1.1.1	eni- [ID]	ins- [ID]	-	vpc- [ID]	sub- [ID] pub- [ID]	2022-06-18 09:17:28	绑定弹性IP 解绑弹性IP 释放

4. 在弹出的释放确认对话框中，单击确认完成 HAVIP 的释放。

## 弹性网卡

最近更新时间：2022-06-16 18:52:33

**弹性网卡 (Elastic Network Interface, ENI)** 是绑定私有网络内云服务器的一种弹性网络接口，可在多个云服务器间自由迁移，弹性网卡常用于配置管理网络与搭建高可靠网络方案。

您可以在云服务器上绑定多个弹性网卡（仅可绑定相同可用区下的弹性网卡，具体绑定数量由服务器规格决定），实现高可用网络方案；也可以在弹性网卡上绑定多个内网 IP，实现单主机多 IP 部署。

关于弹性网卡的常用操作，请参见：

- [创建弹性网卡](#)
- [绑定和配置云服务器](#)
- [解绑云服务器](#)
- [删除弹性网卡](#)
- [申请辅助内网 IP](#)
- [释放辅助内网 IP](#)
- [绑定弹性公网 IP](#)
- [解绑弹性公网 IP](#)
- [修改主内网 IP](#)
- [修改所属子网](#)
- [申请和释放 IPv6](#)

## 共享带宽包

最近更新时间：2023-04-26 12:33:04

共享带宽包（Bandwidth Package, BWP）是一种多 IP 聚合的计费模式，可大幅降低公网费用。当业务中公网流量高峰分布在不同时间段内，可通过共享带宽包实现带宽聚合计费，相比单独为每台设备购买带宽，可帮您节省带宽费用。

共享带宽包提供 [预付费](#)，后付费（[后付费日结](#)、[后付费月结](#)）两类计费模式，满足您不同业务场景。

### ① 说明

如需使用后付费 - 月 TOP5计费共享带宽包，请联系您的商务经理申请开通。

关于共享带宽包的常用操作，请参见：

- [查看计费带宽值](#)
- [下载用量明细](#)
- [修改付费类型](#)
- [管理 IP 带宽包](#)
- [管理设备带宽包](#)

## 共享流量包

最近更新时间：2023-11-24 15:46:21

**共享流量包**（Traffic Package, TP）是一种预付费公网流量套餐，可自动抵扣多种产品的流量消耗。相比后付费流量，共享流量包单价更低，支持统一查看、分析、管理流量用量，帮助您降低网络成本、简化预算管理。

关于共享流量包的常用操作，请参见：

- [创建共享流量包](#)
- [查看共享流量包](#)
- [退还共享流量包](#)

## 网络连接

# NAT 网关

最近更新时间：2022-06-16 18:17:11

**NAT 网关** 是一种 IP 地址转换服务，提供 SNAT 和 DNAT 能力，可为私有网络（VPC）内的资源提供安全、高性能的 Internet 访问服务。例如，为多个无公网访问能力的云服务器提供外网访问的安全出口。

关于 NAT 网关的常用操作，请参见：

- [快速入门](#)
- [修改 NAT 网关配置](#)
- [管理 NAT 网关的弹性 IP](#)
- [管理 SNAT 规则](#)
- [管理端口转发规则](#)
- [配置指向 NAT 网关的路由](#)

## VPN 连接

最近更新时间：2022-04-01 11:05:08

[VPN 连接](#) 是一种基于网络隧道技术，实现本地数据中心与腾讯云上资源连通的传输服务，它能帮您在 Internet 上快速构建一条安全、可靠的加密通道。

关于VPN 连接的常用操作，请参见：

- [VPN 网关](#)
- [对端网关](#)
- [VPN 通道](#)
- [建立 VPC 到 IDC 的连接（策略路由）](#)
- [建立 VPC 到 IDC 的连接（目的路由）](#)
- [建立 IDC 到云联网的连接](#)

## 专线接入

最近更新时间：2023-03-28 10:37:45

**专线接入** 提供了一种快速安全连接腾讯云与本地数据中心的方法。用户可以通过一条物理专线，一次性打通位于多地域的腾讯云计算资源，实现灵活可靠的混合云部署。

关于专线接入的常用操作，请参见：

- [快速入门](#)
- [管理物理线路](#)
- [管理专线网关](#)
- [管理专用通道](#)
- [IDC 通过云联网上云](#)

## 云联网

最近更新时间：2022-07-22 16:06:18

**云联网**（Cloud Connect Network, CCN）为您提供云上私有网络（VPC）间、VPC与本地数据中心（IDC）间内网互联的服务，具备全网多点互联、路由自主学习、链路选优及故障快速收敛等能力。

关于云联网的常用操作，请参见：

- [同账号网络实例互通](#)
- [跨账号网络实例互通](#)
- [实例管理](#)
- [路由管理](#)
- [带宽管理](#)



## 私有连接

最近更新时间：2023-03-28 10:38:52

**私有连接**（Private Link）提供腾讯云 VPC 通过内网访问同地域其他 VPC 的能力，可以在同账号或者不同账户的跨 VPC 之间快速建立访问连接，相比公网服务，可以节约公网带宽，安全性更高，同时能够大幅简化网络架构。

关于私有连接的常见操作，请参见：

- [快速入门](#)
- [管理终端节点](#)
- [管理终端节点服务](#)
- [跨地域 VPC 间服务共享](#)
- [跨账号 VPC 间服务共享](#)

# 安全管理

## 安全组

### 安全组概述

最近更新时间：2023-11-23 10:40:11

安全组是一种虚拟防火墙，具备有状态的数据包过滤功能，用于设置云服务器、负载均衡、云数据库等实例的网络访问控制，控制实例级别的出入流量，是重要的网络安全隔离手段。您可通过如下视频了解安全组的相关信息。

[观看视频](#)

您可以通过配置安全组规则，允许或禁止安全组内的实例的出流量和入流量。

#### 特点

- 安全组是一个逻辑上的分组，您可以将同一地域内具有相同网络安全隔离需求的云服务器、弹性网卡、云数据库等实例加到同一个安全组内。
- 安全组未添加任何规则时，默认拒绝所有流量，您需要添加相应的允许规则。
- 安全组是有状态的，对于您已允许的入站流量，都将自动允许其流出，反之亦然。
- 您可以随时修改安全组的规则，新规则立即生效。

#### 使用限制

有关安全组的使用限制及配额，详情请参见 [限制说明](#)。

#### 安全组规则

##### 组成部分

安全组规则包括如下组成部分：

- 来源或目标：流量的源（入站规则）或目标（出站规则），可以是单个 IP 地址、IP 地址段，也可以是安全组，具体请参见 [安全组规则](#)。
- 协议类型和协议端口：协议类型如 TCP、UDP 等。
- 策略：允许或拒绝。

##### 规则优先级

- 安全组内规则具有优先级。规则优先级通过规则在列表中的位置来表示，列表顶端规则优先级最高，最先应用；列表底端规则优先级最低。
- 若有规则冲突，则默认应用位置更前的规则。
- 当有流量入/出绑定某安全组的实例时，将从安全组规则列表顶端的规则开始逐条匹配至最后一条。如果匹配某一条规则成功，允许通过，则不再匹配该规则之后的规则。

#### 多个安全组

一个实例可以绑定一个或多个安全组，当实例绑定多个安全组时，多个安全组将按照从上到下依次匹配执行，您可以随时 [调整安全组的优先级](#)。

#### 安全组模板

新建安全组时，您可以选择腾讯云为您提供的两种安全组模板：

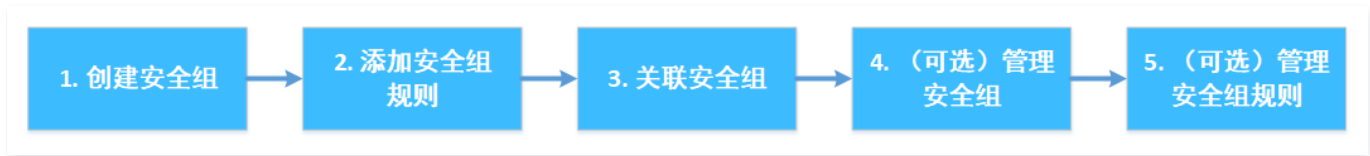
- 放通全部端口模板：将会放通所有出入站流量。
- 放通常用端口模板：将会放通 TCP 22端口（Linux SSH 登录），80、443端口（Web 服务），3389端口（Windows 远程登录）、ICMP 协议（Ping）、放通内网（私有网络网段）。

##### 说明

- 如果提供的安全组模板不满足您的实际使用，您也可以新建自定义安全组，详情请参见 [创建安全组](#)、[安全组应用案例](#)。
- 如果您对应用层（HTTP/HTTPS）有安全防护需求，可另行购买 [腾讯云 Web 应用防火墙（WAF）](#)，WAF 将为您提供应用层 Web 安全防护，抵御 Web 漏洞攻击、恶意爬虫和 CC 攻击等行为，保护网站和 Web 应用安全。

#### 使用流程

安全组的使用流程如下图所示：



## 安全组实践建议

### 创建安全组

- 调用 API 购买 CVM 时建议指定安全组，未指定安全组时，将使用系统自动生成的默认安全组，默认安全组不可删除，默认规则为放通所有 IPv4 规则，创建后可按需修改。
- 实例防护策略有变更，建议优先修改安全组内规则，不需要重新新建一个安全组。

### 管理规则

- 需要修改规则时可以先将当前安全组导出备份，如果新规则有不利影响，可以导入之前的安全组规则进行恢复。
- 当所需规则条目较多时可以使用 [参数模板](#)。

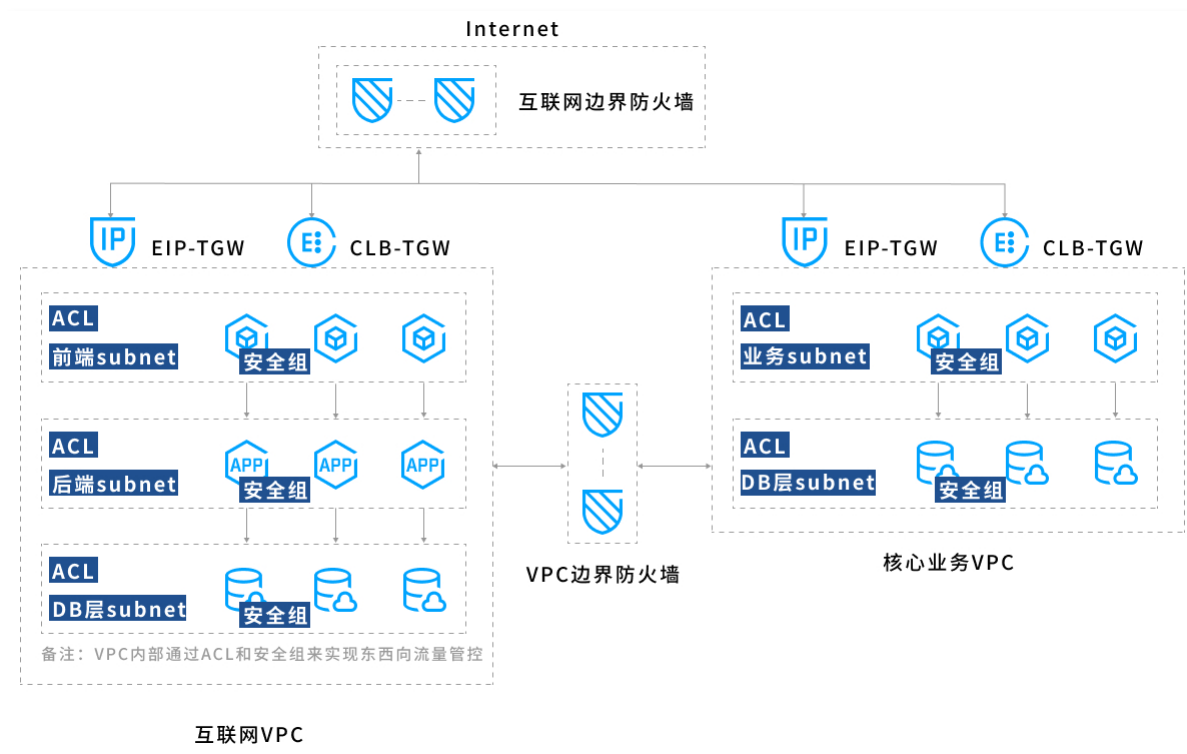
### 关联安全组

- 您可以将有相同防护需求的实例加入一个安全组，而无需为每一个实例都配置一个单独的安全组。
- 不建议一个实例绑定过多安全组，不同安全组规则的冲突可能导致网络不通。

## 安全组和云防火墙

腾讯云云防火墙（Cloud Firewall, CFW），是腾讯云原生的 SaaS 化防火墙产品，并集成了攻击者视角的漏洞扫描能力、IPS 入侵拦截能力、全网威胁情报和高级威胁溯源分析能力，是云环境的流量安全中心和策略管控中心，业务上云的第一道安全门户。

在实际使用场景中，安全组一般部署在 CVM 等云产品边界，用于实现云产品所属安全组间的访问控制。而腾讯云云防火墙部署在 VPC 间的边界或互联网边界，用于实现 VPC 间或腾讯云到互联网访问控制。具体如下图所示：



在如下场景中，使用安全组不能满足需求，可采用 [腾讯云云防火墙](#) 来实现访问控制：

- 了解 CVM 资产在互联网的暴露及漏洞情况，并通过 IPS 入侵防御功能和虚拟补丁功能，对网络漏洞加强防护。
- 按域名实现主动外联控制，加强业务的安全性。
- 按区域实现访问控制，例如，一键查封境外 IP 的访问。

## 创建安全组

最近更新时间：2024-03-20 17:08:41

### 操作场景

安全组是云服务器实例的虚拟防火墙，每台云服务器实例必须至少属于一个安全组。在您创建云服务器实例时，如果您还未创建过安全组，腾讯云提供了“[放通全部端口](#)”和“[放通22, 80, 443, 3389端口和 ICMP 协议](#)”两种模板为您创建一个默认安全组。更多详情，请参见 [安全组概述](#)。您可通过如下视频了解如何创建安全组。

[观看视频](#)

如果您不希望云服务器实例加入默认安全组，您还可以根据本文描述，自行创建安全组。本文指导您在云服务器控制台上创建一个安全组。

### 操作步骤

1. 登录 [安全组控制台](#)，进入安全组管理页面。
2. 在安全组管理页面上方，选择地域，单击新建。
3. 在新建安全组对话框中，完成以下配置。如下图所示：

- **模板**：根据安全组中的云服务器实例需要部署的服务，选择合适的模板，简化安全组规则配置。如下表所示：

模板	说明	场景
放通全部端口	默认放通全部端口到公网和内网，具有一定安全风险。	-
放通22, 80, 443, 3389端口和 ICMP 协议	默认放通22, 80, 443, 3389端口和 ICMP 协议，内网全放通。	安全组中的实例需要部署 Web 服务。
自定义	安全组创建成功后，按需自行添加安全组规则。具体操作请参见 <a href="#">添加安全组规则</a> 。	-

- **名称**：自定义设置安全组名称。
  - **所属项目**：默认选择“默认项目”，可指定为其他项目，便于后期管理。
  - **备注**：自定义，简短地描述安全组，便于后期管理。
  - **高级选项**：可在高级选项中为安全组配置标签，默认无标签。可按需进行添加，标签详情请参见 [标签产品文档](#)。
4. 单击**确定**，完成安全组的创建。  
如果新建安全组时选择了“自定义”模板，创建完成后可单击**立即设置规则**，进行 [添加安全组规则](#)。

# 添加安全组规则

最近更新时间：2024-04-03 16:01:31

## 操作场景

安全组用于管理是否放行来自公网或者内网的访问请求。为安全起见，安全组入方向大多采取拒绝访问策略。如果您在创建安全组时选择了“放通全部端口”模板或者“放通22, 80, 443, 3389端口和 ICMP 协议”模板，系统将会根据选择的模板类型给部分通信端口自动添加安全组规则。更多详情，请参见 [安全组概述](#)。本文指导您通过添加安全组规则，允许或禁止安全组内的云服务器实例对公网或私网的访问。

## 注意事项

- 安全组规则支持 IPv4 安全组规则和 IPv6 安全组规则。
- 一键放通已经包含了 IPv4 安全组规则和 IPv6 安全组规则。

## 前提条件

- 您已经创建一个安全组。具体操作请参见 [创建安全组](#)。
- 您已经知道云服务器实例需要允许或禁止哪些公网或内网的访问。更多安全组规则设置的相关应用案例，请参见 [安全组应用案例](#)。

## 操作步骤

- 登录 [安全组控制台](#)，进入安全组管理页面。
- 在安全组管理页面，选择地域，找到需要设置规则的安全组。
- 在需要设置规则的安全组行中，单击操作列的修改规则。
- 在安全组规则页面，单击入站规则，并根据实际需求选择以下任何一种方式完成操作。



**说明：**

以下操作以方式二：添加规则为例。

- 方式一：一键放通，适用于无需设置 ICMP 协议规则，并通过22, 3389, ICMP, 80, 443, 20, 21端口便能完成操作的场景。
- 方式二：添加规则，适用于需要设置多种通信协议的场景，例如 ICMP 协议。

- 在弹出的添加入站规则窗口中，设置规则。



添加规则的主要参数如下：

- 类型：默认选择“自定义”，您也可以选择其他系统规则模板，例如“Windows 登录”模板、“Linux 登录”模板、“Ping”模板、“HTTP(80)”模板和“HTTPS(443)”模板。
- 来源：流量的源（进站规则）或目标（出站规则），请指定以下选项之一：

来源	说明
IP 地址或 CIDR 段	用 CIDR 表示法（IPV4；如203.0.113.0、203.0.113.0/24或者0.0.0.0/0，其中0.0.0.0/0代表匹配所有 IPv4 地址。IPV6：如FF05::B5、FF05:B5::/60、::/0或者0::0/0，其中::/0或者0::0/0代表匹配所有 IPv6 地址）。
参数模板-IP 地址	引用 <a href="#">参数模板</a> 中的 IP 地址对象。
参数模板-IP 地址组	引用 <a href="#">参数模板</a> 中的 IP 地址组对象。
安全组	引用安全组 ID，您可以引用以下安全组的 ID： <ul style="list-style-type: none"> <li>● 当前安全组：当前安全组表示与云服务器关联的安全组 ID。</li> <li>● 其他安全组：其他安全组表示同一区域中同一项目下的另一个安全组 ID。</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p><b>说明：</b></p> <ul style="list-style-type: none"> <li>● 引用安全组 ID 法作为高阶功能，您可选择使用。所引用安全组的规则不会被添加到当前安全组。</li> <li>● 在配置安全组规则时，如果在来源/目标中输入安全组 ID，表示仅将此安全组 ID 所绑定的云服务器实例、弹性网卡的内网 IP 地址作为来源/目标，不包括外网 IP 地址。</li> </ul> </div>

**说明：**

IP 地址后面的“/数字”为子网掩码，其中数字表示子网掩码中网络位的长度。例如，192.168.0.0/24表示一个网段，子网掩码“/24”表示192.168.0.0的前24位为网络位，后8位为主机位，即在192.168.0.0/24子网内，可分配的主机 IP 范围为：192.168.0.0 - 192.168.0.255。

- 协议端口：填写协议类型和端口范围，协议类型支持 TCP、UDP、ICMP、ICMPv6 及 GRE，协议端口您可以引用 [参数模板](#) 中的协议端口或协议端口组。
- 策略：默认选择“允许”。
  - 允许：放行该端口相应的访问请求。
  - 拒绝：直接丢弃数据包，不返回任何响应信息。
  - 备注：自定义，简短地描述规则，便于后期管理。

6. 单击**确定**，完成安全组进站规则的添加。

7. 在安全组规则页面，单击**出站规则**，并参考 [步骤4](#) - [步骤7](#)，完成安全组出站规则的添加。

# 关联实例至安全组

最近更新时间：2023-10-27 14:27:33

## 说明

安全组支持关联云服务器、弹性网卡、云数据库 MySQL 和负载均衡等，本文以关联云服务器为例。

## 操作场景

安全组用于设置单台或多台云服务器实例的网络访问控制，是重要的网络安全隔离手段。您可以根据业务需要，将云服务器实例关联一个或多个安全组。下面将指导您如何在控制台上将云服务器实例关联安全组。

## 前提条件

已创建云服务器实例。

## 操作步骤

1. 登录 [安全组控制台](#)，进入安全组管理页面。
2. 在[安全组管理](#)页面，选择实例所在地域，找到需要设置规则的安全组。
3. 在需要设置规则的安全组行中，单击操作列的[管理实例](#)，进入关联实例页面。
4. 在关联实例页面，单击[新增关联](#)。
5. 在弹出的“新增实例关联”窗口中，勾选安全组需要绑定的实例，单击[确定](#)。

## 后续操作

- 如果您想查看您在某个地域下创建的所有安全组，您可以查询安全组列表。  
具体操作请参见 [查看安全组](#)。
- 如果您不希望您的云服务器实例属于某个或某几个安全组，您可以将云服务器实例移出安全组。  
具体操作请参见 [移出安全组](#)。
- 如果您的业务不再需要一个或多个安全组，您可以删除安全组。安全组删除后，该安全组内的所有安全组规则将同时被删除。  
具体操作请参见 [删除安全组](#)。

## 安全组修改项目信息

最近更新时间：2024-04-03 16:01:31

### 操作场景

项目功能用于按项目管理云资源，可以对云资源进行分项目管理。创建安全组时必须将安全组分配至项目，腾讯云支持用户在创建安全组后重新将安全组分配至新的项目。

#### 注意：

如果您要将实例分配至新的项目，请先新建项目。具体操作请参考 [新建项目](#)。

### 操作步骤

1. 登录 [安全组控制台](#)。
2. 在安全组的管理页面，选中安全组列表中需要被重新分配至新项目的安全组，选择左上角的**分配至项目**。如下图所示：



3. 在弹出的**分配至项目**窗口中，选择新的项目名称，单击**确定**，即可完成分配至项目的操作。



#### 注意：

切换项目，安全组的鉴权策略会发生变化，需要按照项目信息合理规划访问管理权限和项目权限，具体操作请参考 [项目与标签](#)。



## 管理安全组

### 查看安全组

最近更新时间：2023-10-27 14:27:33

#### 操作场景

如果您想查看您在某一个地域下创建的所有安全组，您可以通过以下操作查看安全组列表。

#### 操作步骤

##### 查看所有安全组

1. 登录 [安全组控制台](#)，进入安全组管理页面。
2. 在安全组管理页面，选择地域，即可查看该地域下的所有安全组。

##### 查看指定安全组

您还可以通过安全组管理页面的搜索功能，查看您需要查看的安全组。

1. 登录 [安全组控制台](#)，进入安全组管理页面。
2. 在安全组管理页面，选择地域。
3. 在该地域下安全组列表的右上方，单击搜索文本框，选择以下任一方式查询您需要查看的安全组。
  - 选择安全组 ID，输入安全组 ID，按 **Q**，即可查询到该安全组 ID 对应的安全组。
  - 选择安全组名称，输入安全组名称，按 **Q**，即可查询到该安全组名称对应的安全组。
  - 选择标签，输入标签名称，按 **Q**，即可查询到该标签下所有的安全组。
  - 选择关键字，输入关键字信息，按 **Q**，即可查询到和输入关键字匹配的所有安全组。

#### 其他操作

如需了解更多查看指定安全组的语法，可在搜索文本框中单击 **Q** 查看相关语法。

## 移出安全组

最近更新时间：2023-10-27 14:27:33

您可以根据业务需要，将云服务器实例移出安全组。

### 前提条件

云服务器实例已加入两个或两个以上安全组。

### 操作步骤

1. 登录 [安全组控制台](#)，进入安全组管理页面。
2. 在安全组管理页面，选择地域，找到需要将实例移出的安全组。
3. 在需要将实例移出的安全组行中，单击操作列的**管理实例**，进入关联实例页面。
4. 在关联实例页面，选择需要移出的实例，单击**移出安全组**。
5. 在弹出的提示框中，单击**确定**。

# 克隆安全组

最近更新时间：2024-04-18 10:08:21

## 操作场景

当您满足如下场景时，您可能需要克隆安全组：

- 假设您已经在地域 A 里创建了一个安全组 sg-A，此时您需要对地域 B 里的实例使用与 sg-A 完全相同的规则，您可以直接将 sg-A 克隆到地域 B，而不需要在地域 B 从零开始创建安全组。
- 如果您的业务需要执行一个新的安全组规则，您可以克隆原来的安全组作为备份。

## 注意事项

- 克隆安全组默认只克隆此安全组的入站/出站规则，不克隆与此安全组相关联的实例。
- 克隆安全组支持跨项目、跨地域。
- 安全组规则中存在来源为安全组的规则时，此安全组不支持跨地域克隆。

## 操作步骤

1. 登录 [安全组控制台](#)，进入安全组管理页面。
2. 在安全组管理页面，选择地域，找到需要克隆的安全组。
3. 在需要克隆的安全组行中，单击操作列的更多 > 克隆。
4. 在弹出的克隆安全组窗口中，选择克隆的目标项目和目标地域，填写安全组的新名称，单击确定。

## 删除安全组

最近更新时间：2023-10-27 14:27:33

### 操作场景

如果您的业务已经不再需要一个或多个安全组，您可以删除安全组。安全组删除后，该安全组内所有安全组规则同时被删除。

### 前提条件

请确认待删除的安全组不存在关联的实例。若存在关联的实例，请先将关联实例移出安全组，否则删除安全组操作不可执行。具体操作请参见 [移出安全组](#)。

### 操作步骤

1. 登录 [安全组控制台](#)，进入安全组管理页面。
2. 在[安全组管理](#)页面，选择地域，找到需要删除的安全组。
3. 在需要删除的安全组行中，单击操作列的[更多 > 删除](#)。
4. 在弹出的提示框中，单击[确定](#)。

# 调整安全组优先级

最近更新时间：2024-03-20 17:08:41

## 操作场景

一个云服务器实例可以绑定一个或多个安全组，当云服务器实例绑定多个安全组时，多个安全组将按照优先级顺序（如1、2）依次匹配执行，您可以根据以下操作调整安全组的优先级。

## 前提条件

云服务器实例已加入两个或两个以上安全组。

## 操作步骤

1. 登录 [云服务器控制台](#)。
2. 在实例管理页面，单击云服务器实例 ID，进入详情页面。
3. 选择安全组选项卡，进入安全组管理页面。
4. 在“已绑定安全组”模块中，单击排序。



5. 单击如下图标，并上下拖动，调整安全组的优先级，位置越靠上，安全组的优先级越高。



6. 完成调整后，单击保存即可。

# 管理安全组规则

## 查看安全组规则

最近更新时间：2023-10-27 14:27:33

### 操作场景

添加安全组规则后，您可以在控制台上查看安全组规则的详细信息。

### 前提条件

已创建安全组，并已在该安全组中添加了安全组规则。

如何创建安全组和添加安全组规则，请参见 [创建安全组](#) 和 [添加安全组规则](#)。

### 操作步骤

1. 登录 [安全组控制台](#)，进入安全组管理页面。
2. 在安全组管理页面，选择地域，找到需要查看规则的安全组。
3. 单击需要查看规则的安全组 ID/名称，进入安全组规则页面。
4. 在安全组规则页面，单击入站/出站规则页签，可以查看到入站/出站的安全组规则。

# 修改安全组规则

最近更新时间：2023-10-27 14:27:33

## 操作场景

安全组规则设置不当会造成严重的安全隐患，例如安全组规则对特定端口的访问不做限制。您可以通过修改安全组中不合理的安全组规则，保证云服务器实例的网络安全。本文指导您如何修改安全组规则。

## 前提条件

已创建安全组，并已在该安全组中添加了安全组规则。

如何创建安全组和添加安全组规则，请参见 [创建安全组](#) 和 [添加安全组规则](#)。

## 操作步骤

1. 登录 [安全组控制台](#)，进入安全组管理页面。
2. 在安全组管理页面，选择地域，找到需要修改规则的安全组。
3. 在需要修改规则的安全组行中，单击操作列的修改规则，进入安全组规则页面。
4. 在安全组规则页面，根据需要修改安全组规则所属的方向（入站/出站），单击入站/出站规则页签。
5. 找到需要修改的安全组规则，单击操作列的编辑，即可对已有规则进行修改。

### ① 说明

修改安全组规则后无需重启云服务器。

# 删除安全组规则

最近更新時間：2023-10-27 14:27:34

## 操作場景

如果您不再需要某個安全組規則，可以刪除安全組規則。

## 前提條件

- 已創建安全組，並已在該安全組中添加了安全組規則。  
如何創建安全組和添加安全組規則，請參見 [創建安全組](#) 和 [添加安全組規則](#)。
- 已確認云服务器实例不需要允許/禁止哪些公网訪問或內網訪問。

## 操作步驟

- 登錄 [安全組控制台](#)，進入安全組管理頁面。
- 在安全組管理頁面，選擇地域，找到需要刪除規則的安全組。
- 在需要刪除規則的安全組行中，單擊操作列的修改規則，進入安全組規則頁面。
- 在安全組規則頁面，根據需要刪除安全組規則所屬的方向（入站/出站），單擊入站/出站規則頁簽。
- 找到需要刪除的安全組規則，單擊操作列的刪除。
- 在彈出的提示框中，單擊確定。



# 导入安全组规则

最近更新時間：2023-10-31 16:30:11

## 操作場景

安全組規則支持導入功能。您可以將導出的安全組規則文件導入到安全組中，快速創建或恢復安全組規則。

## 操作步驟

1. 登錄 [安全組控制台](#)，進入安全組管理頁面。
2. 在安全組管理頁面，選擇地域，找到需要導入規則的安全組。
3. 单击需要導入規則的安全組 ID/名稱，進入安全組規則頁面。
4. 在安全組規則頁面，根據需要導入安全組規則所屬的方向（入站/出站），单击入站/出站規則頁簽。
5. 在入站/出站規則頁簽下，单击導入規則。
6. 在彈出的批量導入-入站/出站規則窗口中，選擇導入方式和已編輯好的入站/出站規則模板文件，单击開始導入。

### ① 說明

- 如果將安全組下的安全組規則全部替換，您可選擇覆蓋導入，用文件中的安全組規則替換安全組中原有的所有規則。此方式影響較大，仔細檢查文檔是否準確，同時進行安全組快照。
- 如果將規則的安全組下已存在安全組規則，您可選擇追加導入，選擇文件中規則將添加至原有規則前。
- 如果將規則的安全組下沒有安全組規則，建議您先下載模板，待編輯好模板文件後，再將文件導入。
- 導入規則模板文件中來源和協議端口格式可參照控制台頁面提示。


## 导出安全组规则

最近更新时间：2023-10-27 14:27:34

### 操作场景

安全组规则支持导出功能，您可以将安全组下的安全组规则导出，用于本地备份。

### 操作步骤

1. 登录 [安全组控制台](#)，进入安全组管理页面。
2. 在安全组管理页面，选择地域，找到需要导出规则的安全组。
3. 单击需要导出规则的安全组 ID/名称，进入安全组规则页面。
4. 在安全组规则页面，根据需要导出安全组规则所属的方向（入站/出站），单击入站/出站规则页签。
5. 在入站/出站规则页签下，单击右上方的 ，下载并保存安全组规则文件至本地。

# 排序安全组规则

最近更新时间：2024-04-03 16:01:31

## 操作场景

一个安全组中可以添加多条安全组规则，安全组规则按照由上到下的顺序匹配生效，您可以根据业务需要对安全组规则进行排序调整。

## 前提条件

已创建安全组及安全组规则，且至少有条或两条以上安全组规则，详情请参见 [添加安全组规则](#)。

## 操作步骤

1. 登录 [安全组控制台](#)，进入安全组管理页面。
2. 在安全组管理页面，选择地域。
3. 找到需要修改规则的安全组，单击“安全组 ID”，或单击操作列的修改规则，进入安全组规则页面。



4. 在安全组规则页面，单击[优先级排序](#)。



5. 您可以拖动如下图标，对安全组规则顺序进行排序，位置越靠上，安全组规则的优先级越高。调整完成后单击保存即可。

来源 ⓘ	协议端口 ⓘ	策略
0.0.0.0/0	ICMP	允许
0.0.0.0/0	TCP:22	允许
0.0.0.0/0	TCP: [REDACTED]	允许
0.0.0.0/0	UDP: [REDACTED]	允许
10 [REDACTED].0/16	ALL	允许
192 [REDACTED].0/16	ALL	允许

共 6 条

# 快照回滚

最近更新时间：2023-10-27 14:27:34

如安全组配置了快照策略，则安全组规则将按照设定的快照策略进行规则的备份。当需要将安全组规则恢复到备份的某个规则状态时，可执行快照回滚操作。

## 前提条件

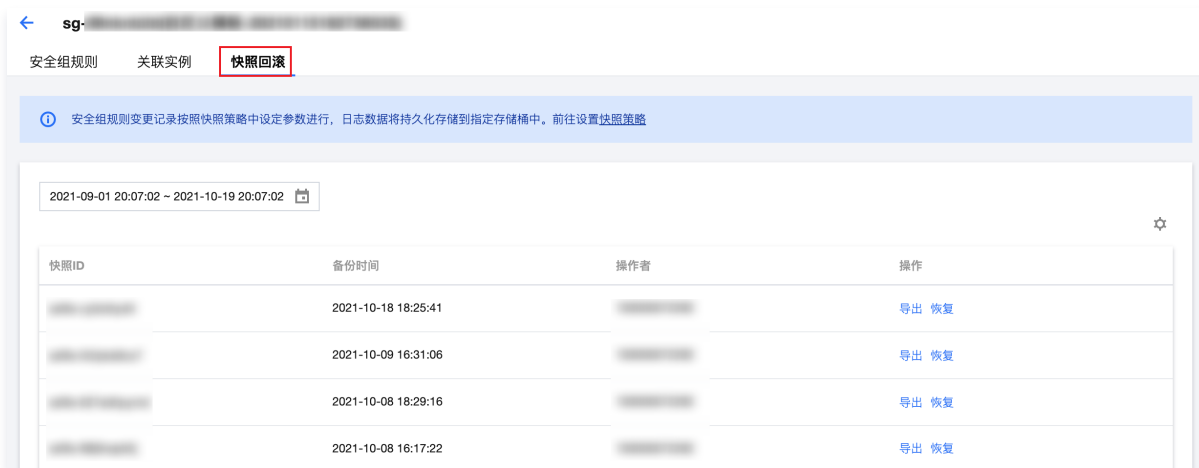
安全组配置 [快照策略](#)，且至少完成了一次快照备份。

## 操作步骤

1. 登录 [安全组控制台](#)，进入安全组管理页面。
2. 在安全组管理页面，单击需要回滚规则的安全组 ID，进入安全组详情界面。
3. 单击快照回滚页签，界面将按时间展示所有快照记录，默认展示7天内容，可自定义设置查询快照记录的时间区间。

### ① 说明

如果备份记录较多，建议一次性查询不要超过三个月，否则可能导致系统响应较慢。



4. 单击导出可导出该次快照记录的安全组出入站规则信息，分别保存在出站规则和入站规则文件中。
5. 单击恢复，进入恢复安全组界面，同时展示安全组规则预览及规则比对内容。

### ① 说明

- 图中 + 号标识的是快照备份记录中相比当前安全组规则新增的规则条目，- 为删除的条目。注意，当前比对界面，是以此刻选择比对预览的时刻为准，如在此期间进行规则变更，比对校验可能不准确。
- 恢复安全组时，若其来源中包含参数模板规则及嵌套安全组，参数模板内规则以及安全组关联实例以当前状态为准。
- 安全组恢复操作等同导入，恢复后将以覆盖方式取代当前所有规则，请谨慎操作。

恢复安全组
✕

**ⓘ** 安全组恢复操作等同导入，恢复后将以覆盖方式取代当前所有规则，请谨慎操作。  
当前规则以选择对比操作时间为准，如您在此期间进行规则变更，规则变更校验可能不准确。

**安全组规则预览**

入站规则    出站规则

**当前规则**

来源	协议端口	策略	备注
- 0.0.0.0/0	ICMP	允许	放通Ping服务
0.0.0.0/0	ICMPv6	允许	放通Ping服务
- 0.0.0.0/0	TCP:22	允许	放通Linux SS...
0.0.0.0/0	TCP:22	允许	放通Linux SS...
0.0.0.0/0	TCP:3389	允许	放通Window...
0.0.0.0/0	TCP:3389	允许	放通Window...
10.0.0.0/24	ALL	允许	放通内网 (云...
172.16.0.0/16	ALL	允许	放通内网 (云...
192.168.0.0/16	ALL	允许	放通内网 (云...

共 9 条    10 条 / 页    1 / 1 页

**恢复规则**

来源	协议端口	策略	备注
+ 0.0.0.0/0	ICMP	拒绝	放通Ping服务
0.0.0.0/0	ICMPv6	允许	放通Ping服务
+ 0.0.0.0/0	TCP:22	拒绝	放通Linux SS...
0.0.0.0/0	TCP:22	允许	放通Linux SS...
0.0.0.0/0	TCP:3389	允许	放通Window...
0.0.0.0/0	TCP:3389	允许	放通Window...
10.0.0.0/24	ALL	允许	放通内网 (云...
172.16.0.0/16	ALL	允许	放通内网 (云...
192.168.0.0/16	ALL	允许	放通内网 (云...

共 9 条    10 条 / 页    1 / 1 页

规则变更数 新增规则 2 条 删除规则 2 条

6. 确认无误后单击**确定**完成安全组规则的回滚。

## 安全组应用案例

最近更新时间：2023-12-28 11:08:11

安全组的设置用来管理云服务器是否可以被访问，您可以通过配置安全组的入站和出站规则，设置您的服务器是否可以被访问以及访问其他网络资源。

默认情况下，安全组的入站规则和出站规则如下：

- 为了数据安全，安全组的入站规则为拒绝策略，禁止外部网络的远程访问。如果您需要您的云服务器被外部访问，则需要放通相应端口的入站规则。
- 安全组的出站规则用于设置您的云服务器是否可以访问外部网络资源。如果您选择“放通全部端口”或“放通22, 80, 443, 3389端口和 ICMP 协议”，则安全组出站规则为全部放通，入站规则与安全组名称放通的内容一致。如果您选择自定义安全组规则，出站规则默认为全部拒绝，您需要放通相应端口的出站规则来访问外部网络资源。

### 常见应用场景

本文介绍了几个常见的安全组应用场景，如果以下场景可以满足您的需求，可直接按照场景中的推荐配置进行安全组的设置。

#### 场景一：允许 SSH 远程连接 Linux 云服务器

案例：您创建了一台 Linux 云服务器，并希望通过 SSH 远程连接到云服务器。

解决方法：添加入站规则时，在“类型”中选择“Linux 登录”，开通22号协议端口，放通 Linux SSH 登录。

您还可以根据实际需求，放通全部 IP 或指定 IP（IP 段），配置可通过 SSH 远程连接到云服务器的 IP 来源。

方向	类型	来源	协议端口	策略
入方向	Linux 登录	全部 IP: 0.0.0.0/0 指定 IP: 输入您指定的 IP 或 IP 段	TCP:22	允许

#### 场景二：允许 RDP 远程连接 Windows 云服务器

案例：您创建了一台 Windows 云服务器，并希望通过 RDP 远程连接到云服务器。

解决方法：添加入站规则时，在“类型”中选择“Windows 登录”，开通3389号协议端口，放通 Windows 远程登录。

您还可以根据实际需求，放通全部 IP 或指定 IP（IP 段），配置可通过 RDP 远程连接到云服务器的 IP 来源。

方向	类型	来源	协议端口	策略
入方向	Windows 登录	全部 IP: 0.0.0.0/0 指定 IP: 输入您指定的 IP 或 IP 段	TCP:3389	允许

#### 场景三：允许公网 Ping 服务器

案例：您创建了一台云服务器，希望可以测试这台云服务器和其他云服务器之间的通信状态是否正常。

解决方法：使用 ping 程序进行测试。即在添加入站规则时，将“类型”选择为“Ping”，开通 ICMP 协议端口，允许其他云服务器通过 ICMP 协议访问该云服务器。

您还可以根据实际需求，放通全部 IP 或指定 IP（IP 段），配置允许通过 ICMP 协议访问该云服务器的 IP 来源。

方向	类型	来源	协议端口	策略
入方向	Ping	全部 IP: 0.0.0.0/0 指定 IP: 输入您指定的 IP 或 IP 地址段	ICMP	允许

#### 场景四：Telnet 远程登录

案例：您希望通过 Telnet 远程登录云服务器。

解决方法：如需通过 Telnet 远程登录云服务器，则需在添加入站规则时，配置以下安全组规则：

方向	类型	来源	协议端口	策略
入方向	自定义	全部 IP: 0.0.0.0/0 指定 IP: 输入您指定的 IP 或 IP 地址段	TCP:23	允许

#### 场景五：放通 Web 服务 HTTP 或 HTTPS 访问

案例：您搭建了一个网站，希望用户可以通过 HTTP 或者 HTTPS 的方式访问您搭建的网站。

解决方法：如需通过 HTTP 或者 HTTPS 的方式访问网站，则需在添加入站规则时，根据实际需求配置以下安全组规则：

- 允许公网上的所有 IP 访问该网站

方向	类型	来源	协议端口	策略
入方向	HTTP (80)	0.0.0.0/0	TCP:80	允许
入方向	HTTPS (443)	0.0.0.0/0	TCP:443	允许

- 允许公网上的部分 IP 访问该网站

方向	类型	来源	协议端口	策略
入方向	HTTP (80)	允许访问您网站的 IP 或 IP 地址段	TCP:80	允许
入方向	HTTPS (443)	允许访问您网站的 IP 或 IP 地址段	TCP:443	允许

### 场景六：允许外部 IP 访问指定端口

**案例：**您部署业务后，希望指定的业务端口（例如：1101）可以被外部访问。

**解决方法：**添加入站规则时，在“类型”中选择“自定义”，开通1101号协议端口，允许外部访问指定的业务端口。

您还可以根据实际需求，放通全部 IP 或指定 IP（IP 段），允许访问指定的业务端口的 IP 来源。

方向	类型	来源	协议端口	策略
入方向	自定义	全部 IP：0.0.0.0/0 指定 IP：输入您指定的 IP 或 IP 地址段	TCP:1101	允许

### 场景七：拒绝外部 IP 访问指定端口

**案例：**您部署业务后，希望指定的业务端口（例如：1102）不被外部访问。

**解决方法：**添加入站规则时，在类型中选择自定义，配置1102号协议端口，将策略设置为拒绝，拒绝外部访问指定的业务端口。

方向	类型	来源	协议端口	策略
入方向	自定义	全部 IP：0.0.0.0/0 指定 IP：输入您指定的 IP 或 IP 地址段	TCP:1102	拒绝

### 场景八：只允许云服务器访问特定外部 IP

**案例：**您希望您的云服务器只能访问外部特定的 IP 地址。

**解决方法：**参考如下配置，增加如下两条出方向的安全组规则。

- 允许实例访问特定公网 IP 地址
- 禁止实例以任何协议访问所有公网 IP 地址

#### ⚠ 注意

允许访问的规则优先级应高于拒绝访问的规则优先级。

方向	类型	来源	协议端口	策略
出方向	自定义	允许云服务器访问的特定公网 IP 地址	需使用的协议类型和端口	允许
出方向	自定义	0.0.0.0/0	ALL	拒绝

### 场景九：拒绝云服务器访问特定外部 IP

**案例：**您不希望您的云服务器可以访问外部特定的 IP 地址。

**解决方法：**参考如下配置，添加安全组规则。

方向	类型	来源	协议端口	策略
出方向	自定义	拒绝实例访问的特定公网 IP 地址	ALL	拒绝

### 场景十：使用 FTP 上传或下载文件



**案例：**您需要使用 FTP 软件向云服务器上传或下载文件

**解决方法：**参考如下配置，添加安全组规则。

方向	类型	来源	协议端口	策略
入方向	自定义	0.0.0.0/0	TCP:20-21	允许

## 多场景组合

在实际的场景中，可能需要根据业务需求配置多个安全组规则。例如，同时配置入站或者出站规则。一台云服务器可以绑定一个或多个安全组，当云服务器绑定多个安全组时，多个安全组将按照从上到下依次匹配执行。您可以随时调整安全组的优先级，安全组规则的优先级说明请参考 [规则优先级说明](#)。

## 服务器常用端口

最近更新时间：2024-03-13 17:02:41

如下是服务器常用端口介绍，关于 Windows 下更多的服务应用端口说明，请参考微软官方文档（[Windows 的服务概述和网络端口要求](#)）。

端口	服务	说明
21	FTP	FTP 服务器所开放的端口，用于上传、下载。
22	SSH	22端口就是 SSH 端口，用于通过命令行模式远程连接 Linux 系统服务器。
25	SMTP	SMTP 服务器所开放的端口，用于发送邮件。
80	HTTP	用于网站服务例如 IIS、Apache、Nginx 等提供对外访问。
110	POP3	110端口是为 POP3（邮件协议 3）服务开放的。
137、138、139	NETBIOS 协议	其中137、138是 UDP 端口，当通过网上邻居传输文件时用这个端口。而139端口：通过这个端口进入的连接试图获得 NetBIOS/SMB 服务。这个协议被用于 Windows 文件和打印机共享和 SAMBA。
143	IMAP	143端口主要是用于“Internet Message Access Protocol” v2（Internet 消息访问协议，简称 IMAP），和 POP3 一样，是用于电子邮件的接收的协议。
443	HTTPS	网页浏览端口，能提供加密和通过安全端口传输的另一种 HTTP。
1433	SQL Server	1433端口，是 SQL Server 默认的端口，SQL Server 服务使用两个端口：TCP-1433、UDP-1434。其中1433用于供 SQL Server 对外提供服务，1434用于向请求者返回 SQL Server 使用了哪个 TCP/IP 端口。
3306	MySQL	3306端口，是 MySQL 数据库的默认端口，用于 MySQL 对外提供服务。
3389	Windows Server Remote Desktop Services（远程桌面服务）	3389端口是 Windows Server 远程桌面的服务端口，可以通过这个端口，用“远程桌面”连接工具来连接到远程的服务器。
8080	代理端口	8080端口同80端口，是被用于 WWW 代理服务的，可以实现网页浏览，经常在访问某个网站或使用代理服务器的时候，会加上“:8080”端口号。另外 Apache Tomcat web server 安装后，默认的服务端口就是8080。

# 网络 ACL

## 规则概述

最近更新时间：2023-10-27 14:27:34

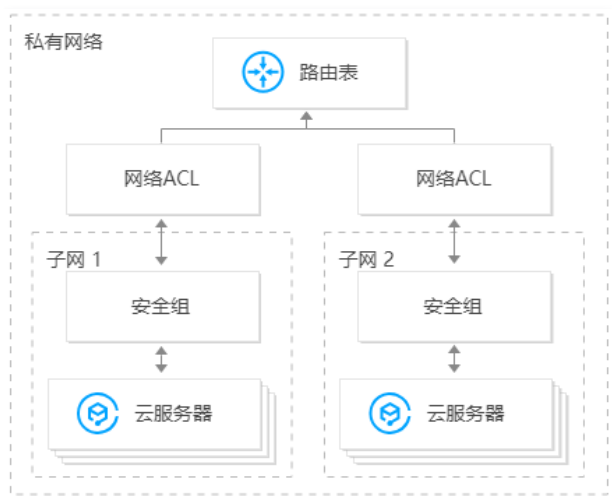
网络访问控制列表（Access Control List, ACL）是一种子网级别的可选安全层，用于控制进出子网的数据流，可以精确到协议和端口粒度。您可以通过如下视频了解使用网络 ACL 实现访问控制的相关规则。

[观看视频](#)

### 使用场景

您可以为具有相同网络流量控制的子网关联同一个网络 ACL，通过设置出站和入站规则，对进出子网的流量进行精确控制。

例如，您在腾讯云私有网络内托管多层 Web 应用，创建了不同子网分别部署 Web 层、逻辑层和数据层服务，通过网络 ACL，您可以控制这三个子网之间的访问，使得：Web 层子网和数据层子网无法相互访问，只有逻辑层可以访问 Web 层和数据层子网。



### ACL 规则

当您在网络 ACL 中添加或删除规则后，会自动应用到与其相关联的子网的网络流量控制。

网络 ACL 规则包含入站规则和出站规则，规则组成如下：

- 源 IP/目标 IP：流量的源/目标 IP。如果是入站规则，需要输入源 IP；如果是出站规则，需要输入目标 IP，源/目标 IP 均支持以下格式：
  - 单个 IP：例如 192.168.0.1 或 FF05::B5
  - CIDR：例如 192.168.1.0/24 或 FF05:B5::/60
  - 所有 IPv4：0.0.0.0/0
  - 所有 IPv6：0::0/0 或 ::/0
- 协议类型：选择 ACL 规则允许/拒绝的协议类型，例如 TCP、UDP 等。
- 端口：流量的来源/目标端口，端口支持以下格式：
  - 单个端口：例如 22 或 80
  - 连续端口：例如 1-65535 或 100-20000
  - 所有端口：ALL
- 策略：允许或拒绝。

### 默认规则

每个网络 ACL 在创建后都将包含两条默认规则，默认规则无法修改或删除，且优先级最低。

- 入方向默认规则

协议类型	端口	源 IP	策略	说明
ALL	ALL	0.0.0.0/0	拒绝	拒绝所有入站流量

- 出方向默认规则

协议类型	端口	目标 IP	策略	说明
------	----	-------	----	----

ALL	ALL	0.0.0.0/0	拒绝	拒绝所有出站流量
-----	-----	-----------	----	----------

### 规则优先级

- 网络 ACL 规则的优先级通过规则在列表中的位置来表示，列表顶端的规则优先级最高，最先应用；列表底端的规则优先级最低。
- 若有规则冲突，则默认应用位置更前的规则。
- 当绑定了网络 ACL 的子网有流量入/出时，将从网络 ACL 列表顶端的规则开始逐条匹配至最后一条。如果匹配某一条规则成功，则允许通过，不再匹配该规则之后的规则。

### 应用示例

假设某子网关联了网络 ACL，该子网允许所有源 IP 访问子网内云服务器的所有端口，同时拒绝源 IP 为192.168.200.11/24的 HTTP 服务访问80端口。根据上述要求，其关联的网络 ACL 应添加如下两条入站规则：

协议类型	端口	源 IP	策略	说明
HTTP	80	192.168.200.11/24	拒绝	拒绝该 IP 的 HTTP 服务访问80端口
ALL	ALL	0.0.0.0/0	允许	允许所有源 IP 访问所有端口

### 安全组与网络 ACL 的区别

对比项	安全组	网络 ACL
流量控制	云服务器、数据库等实例级别的流量访问控制	子网级别的流量控制
规则	支持允许规则、拒绝规则	支持允许规则、拒绝规则
有无状态	有状态：返回数据流会被自动允许，不受任何规则的影响	无状态：返回数据流必须被规则明确允许
生效时间	只有在创建云服务器、云数据库等实例时指定安全组，或实例创建后再关联安全组，规则才会被应用到实例	创建 ACL 并绑定子网后，ACL 将自动应用到关联子网内的所有云服务器、云数据库等实例
规则优先级	有规则冲突时，默认应用位置更前的规则	有规则冲突时，默认应用位置更前的规则

## 限制说明

最近更新时间：2023-10-27 14:27:34

### 使用限制

- 一个网络 ACL 可以绑定多个子网。
- 网络 ACL 没有任何状态，您需要分别设置出站规则和进站规则。
- 网络 ACL 不会影响所关联子网内的 CVM 实例之间的内网互通。

### 配额限制

资源	限制
每个私有网络内网络 ACL 数	50个
每个网络 ACL 中规则数	<ul style="list-style-type: none"><li>• 进站方向：20条</li><li>• 出站方向：20条</li></ul>
每个子网关联的网络 ACL 个数	1个

## 管理网络 ACL

最近更新时间：2024-03-20 17:08:41

您可通过如下视频了解配置网络 ACL 实现访问控制的相关信息。

[观看视频](#)

### 创建网络 ACL

1. 登录 [私有网络控制台](#)。
2. 单击左侧目录中的安全 > 网络 ACL，进入管理页面。
3. 在列表上方，选择地域和私有网络，单击+新建。
4. 在弹出框中，输入名称，选择所属的私有网络，单击确定即可。

#### 新建网络 ACL

名称

您还可以输入60个字符

所属网络

[高级选项](#)

5. 在列表页中，单击对应的 ACL ID 即可进入详情页，添加 ACL 规则、关联子网。

### 增加网络 ACL 规则

1. 登录 [私有网络控制台](#)。
2. 单击左侧目录中的安全 > 网络 ACL，进入管理页面。
3. 在列表中，找到需要修改的网络 ACL，单击其 ID，进入详情页。
4. 新增出/入站规则，单击出站规则或入站规则 > 编辑 > 新增一行，选择协议类型并输入端口、源 IP，以及选择策略。
  - 协议类型：选择 ACL 规则允许/拒绝的协议类型，如 TCP、UDP 等。
  - 端口：流量的来源端口，支持单个端口或端口段，如80或90 - 100。
  - 源 IP：流量的源 IP 或源网段，支持 IP 或 CIDR，如 10.20.3.0 或 10.0.0.2/24。
  - 策略：允许或拒绝。

← VPC 网络ACL帮助文档

基本信息 **入站规则** 出站规则

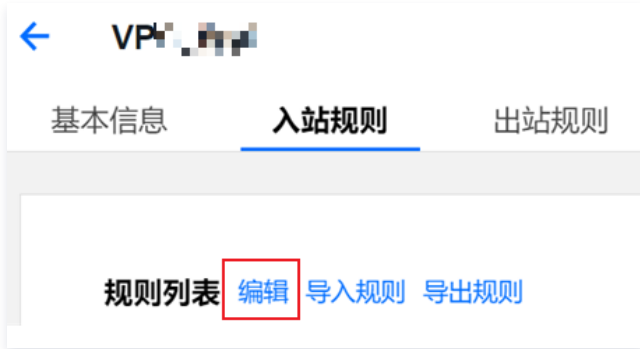
#### 规则列表

源IP	协议类型	端口	策略	备注	操作
<input type="text" value="0.0.0.0"/>	TCP	<input type="text" value=""/>	拒绝	<input type="text" value=""/>	删除
0.0.0.0	all	ALL	拒绝		

5. 单击保存即可。

## 删除网络 ACL 规则

1. 登录 [私有网络控制台](#)。
2. 单击左侧目录中的安全 > 网络 ACL，进入管理页面。
3. 在列表中，找到需要删除的网络 ACL，单击其 ID，进入基本信息页面。
4. 单击入站规则或出站规则选项卡，进入“规则列表”页面。
5. 单击编辑，删除入站规则与删除出站规则步骤一致，本文以删除入站规则为例。



6. 在列表中，找到需要删除的规则所在行，单击操作列下的删除。

**说明：**  
此时本条 ACL 规则置灰。若本次删除属于误操作，您可单击操作列下的恢复删除，将其恢复。

源 IP ①	协议类型	端口 ①	策略	备注	操作
<input type="text"/>	ICMPv6	<input type="text"/>	拒绝	<input type="text"/>	<input type="button" value="删除"/>

7. 单击保存，保存上述操作。

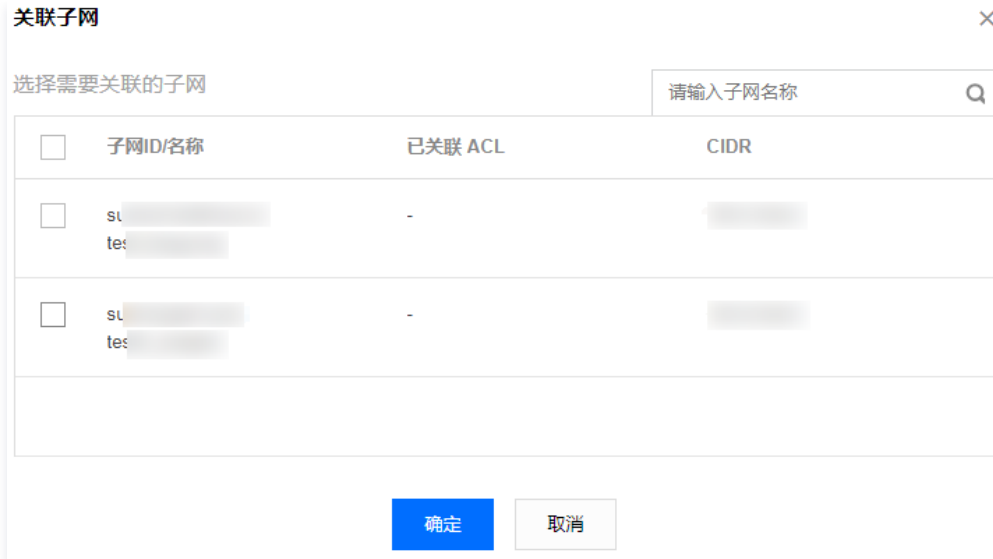
**注意：**  
ACL 规则的删除或恢复删除操作，必须保存后才会生效。

## 子网关联网络 ACL

1. 登录 [私有网络控制台](#)。
2. 单击左侧目录中的安全 > 网络 ACL，进入管理页面。
3. 在列表中，找到需要关联的网络 ACL，单击其 ID，进入详情页。
4. 在基本信息页面的“关联子网”模块，单击新增关联。

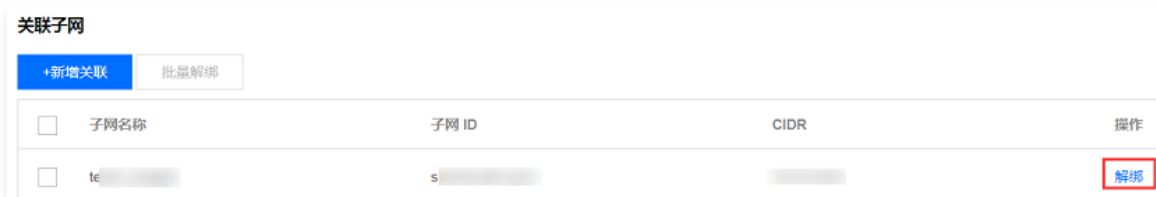


5. 在弹出框中，选择需要关联的子网，单击确定即可。

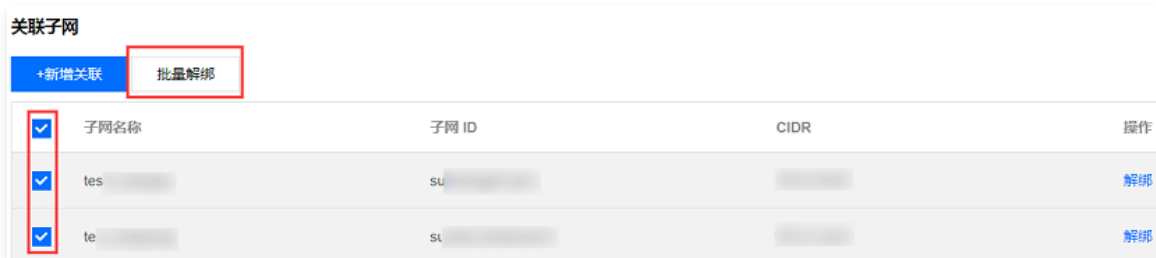


### 子网解除关联网络 ACL

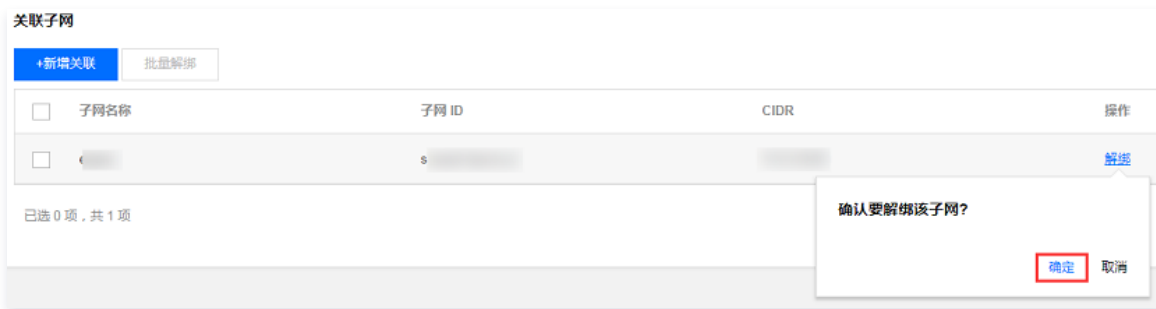
1. 登录 [私有网络控制台](#)。
2. 单击左侧目录中的安全 > 网络 ACL，进入管理页面。
3. 在列表中，找到需要解除关联的网络 ACL，单击其 ID，进入详情页。
4. 解除关联子网有以下方法：
  - 方法一：在基本信息页面的“关联子网”模块，找到需要解除关联的子网，单击解绑。



- 方法二：在基本信息页面的“关联子网”模块，勾选所有需要解除关联的子网，单击批量解绑。



5. 在弹出框中单击确定即可。



### 删除网络 ACL

1. 登录 [私有网络控制台](#)。
2. 单击左侧目录中的安全 > 网络 ACL，进入管理页面。
3. 选择地域和私有网络。



4. 在列表中，找到需要删除的网络 ACL，单击删除并确定操作，即可删除该网络 ACL 及该网络 ACL 的所有规则。

**说明：**

若删除置灰，如下图中的网络 ACL testEg，表示该网络 ACL 正与子网相关联，您需要先解除子网关联后，才能进行删除操作。

网络ACL 华南地区 (广州) 全部私有网络 网络ACL帮助文档

+新建 ID/名称/VPC ID/TAG/标签

ID/名称	关联子网数	所属网络	标签	操作
acl- VPC	1	vpc- VPC	无	<a href="#">关联子网</a> <a href="#">删除</a>
acl- acl	0	vpc- VPC	无	<a href="#">关联子网</a> <a href="#">删除</a>

# 参数模板

## 概述

最近更新时间：2023-10-27 14:27:34

参数模板是一组 IP 地址或协议端口参数的集合，将一组有相同诉求的 IP 地址或协议端口保存为模板，在添加安全组规则时，作为来源/目的 IP、协议端口可直接引用。合理使用参数模板，可以提高您使用安全组的效率。

## 应用场景

参数模板适用于如下场景：

- 统一管理具有相同诉求的 IP / 协议端口组。
- 统一管理具有频繁编辑诉求的 IP / 协议端口组。

## 参数模板类型

腾讯云支持如下四种类型的参数模板：

- IP 地址：也称为 IP 地址对象，是一组 IP 地址的集合，支持单个 IP、CIDR、IP 范围。
- IP 地址组：也称为 IP 地址组对象，是多个 IP 地址对象的集合。
- 协议端口：也称为协议端口对象，是一组协议端口的集合，支持单个端口、多个端口、连续端口及所有端口，协议支持 TCP、UDP、ICMP、GRE 协议。
- 协议端口组：也称为协议端口组对象，是一组协议端口对象的集合。

# 限制说明

最近更新时间：2023-10-27 14:27:34

## 使用限制

- IP 地址模板支持格式
  - 单个 IP，如 10.0.0.1。
  - 连续 IP，如 10.0.0.1 - 10.0.0.100。
  - 网段，如 10.0.1.0/24。
- 端口模板支持格式
  - 单个端口，如 TCP:80。
  - 多个离散端口，如 TCP:80,443。
  - 连续端口，如 TCP:3306-20000。
  - 所有端口，如 TCP:ALL。

## 配额限制

实例	限制（单位：个）
IP 地址对象（ipm）	每个租户上限1000
IP 地址组对象（ipmg）	每个租户上限1000
协议端口对象（ppm）	每个租户上限1000
协议端口组对象（ppmg）	每个租户上限1000
IP 地址对象（ipm）内的 IP 地址成员	每个租户上限20
IP 地址组对象（ipmg）内的 IP 地址对象成员（ipm）	每个租户上限20
协议端口对象（ppm）内的协议端口成员	每个租户上限20
协议端口组对象（ppmg）内的协议端口对象成员（ppm）	每个租户上限20
IP 地址对象（ipm）可被多少个 IP 地址组对象（ipmg）引用	每个租户上限50
协议端口对象（ppm）可被多少个协议端口组对象（ppmg）引用	每个租户上限50

### ① 说明

若参数模板被安全组引用，系统将把参数模板内的 IP/端口转换为多条安全组规则，转换后的安全组规则不超过2000条。

## 管理参数模板

最近更新时间：2024-01-25 15:38:01

本章节介绍如何在控制台创建维护参数模板（IP 地址、IP 地址组、协议端口、协议端口组），及参数模板在安全组中的使用。

### 创建参数模板

#### 创建 IP 地址参数模板

将具有相同诉求或频繁编辑诉求的 IP 加入到该 IP 地址对象中。

#### 操作步骤

1. 登录 [私有网络控制台](#)。
2. 单击左侧目录中的安全 > 参数模板，进入管理页面。
3. 在 IP 地址标签页，单击新建。
4. 在弹出框中，填写名称和 IP 地址，单击确定即可。

IP 地址支持按照如下范围添加多个 IP 地址，请换行分隔，格式如下：

- 单个 IP：如 10.0.0.1 或 FF05::B5。
- CIDR 网段：如 10.0.1.0/24 或 FF05:B5::/60。
- 连续地址段：如10.0.0.1-10.0.0.100。

### 新建 IP 地址

名称

IP 地址 <small>①</small>	备注	操作
<input type="text" value="10.0.0.1"/>	<input type="text"/>	<input type="button" value="✕"/>
<input type="text" value="10.0.1.0/24"/>	<input type="text"/>	<input type="button" value="✕"/>
<input type="text" value="10.0.0.1-10.0.0.100"/>	<input type="text"/>	<input type="button" value="✕"/>

[+ 新增一行](#)

#### 创建 IP 地址组参数模板

可将多个 IP 地址对象添加到一个 IP 地址组中，统一管理。

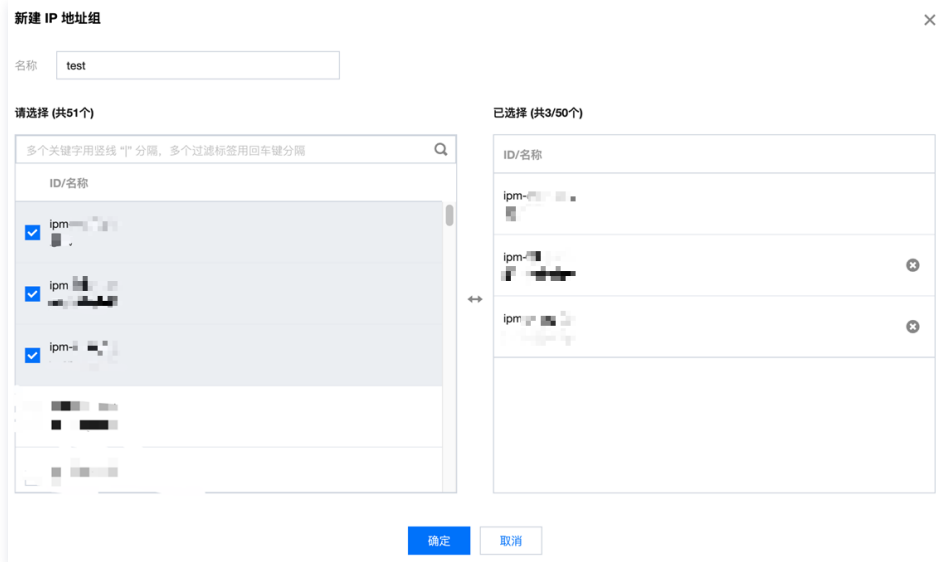
#### 操作步骤

1. 选择IP 地址组标签页，进入管理页面，单击新建。

### 参数模板

IP 地址 **IP 地址组** 协议端口 协议端口组

2. 在弹出框中，填写名称，并选择需要添加的 IP 地址对象，单击确定即可。



### 创建协议端口参数模板

将具有相同诉求或频繁编辑诉求的协议端口加入到该协议端口对象中。

#### 操作步骤

1. 登录 [私有网络控制台](#)。
2. 单击左侧目录中的安全 > 参数模板，进入管理页面。
3. 单击协议端口选项卡，进入协议端口标签页，单击新建。
4. 在弹出框中，填写名称和协议端口，单击确定即可。

协议端口支持按照如下范围添加多个协议端口，请换行分隔，格式如下：

- 单个端口，如 TCP:80 。
- 多个离散端口，如 TCP:80,443 。
- 连续端口，如 TCP:3306-20000 。
- 所有端口，如 TCP:ALL 。



## 创建协议端口组参数模板

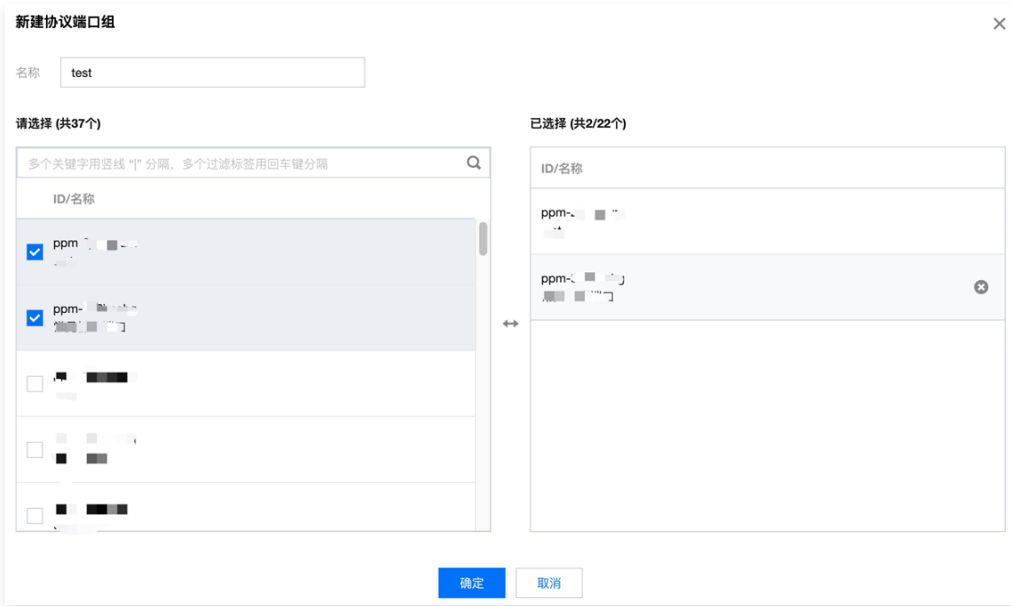
您可将创建的多个协议端口对象同时添加到一个协议端口组中，统一管理。

### 操作步骤

1. 选择协议端口组标签页，进入管理页面，单击新建。



2. 在弹出框中，填写名称和选择需要添加的协议端口对象，单击确定即可。



## 修改参数模板

如需对创建的参数模板进行修改，例如，增加/删除 IP 地址、增加/删除协议端口，可按照如下步骤操作。

### 操作步骤

1. 单击已创建的 IP 地址、IP 地址组、协议端口，或协议端口组参数模板，右侧的编辑，例如，下图为修改 IP 地址对象。



2. 在弹出的编辑对话框中，修改相应参数，并单击确定即可。

## 删除参数模板

如不需要使用参数模板，可将其删除，删除后，所有包含此参数模板的安全组中的策略配置将一同删除，请评估后谨慎操作。

### 操作步骤

1. 单击已创建的参数模板右侧的删除。



2. 删除后，所有包含此 IP 地址、或协议端口的策略将一同删除，确认无误后，在弹出的删除确认框中继续单击**确定**。



### 在安全组中引用参数模板

参数模板创建后，可直接在安全组添加规则时引用参数模板来快速添加 IP 来源或协议端口，提高安全组规则的添加效率。

#### 操作步骤

1. 登录 [私有网络控制台](#)。
2. 单击左侧目录中的安全 > 安全组，进入管理页面。
3. 在列表中，找到需要引用参数模板的安全组，单击其 ID，进入详情页。
4. 在入站 / 出站规则标签页中，单击**添加规则**。
5. 在弹出框中，选择“自定义”类型，在弹框中选择自定义类型，来源分类选择**参数模板-IP地址/参数模板-IP地址组**后，选中对应的IP地址/IP地址组，协议端口分别选择对应的协议端口参数模板，并单击**确定**。添加入站 / 出站规则的详细步骤，请参见 [添加安全组规则](#)。

#### ① 说明

后续如需增加新的 IP 地址或协议端口，仅需在对应 IP 地址组或协议端口组中增加即可，无须修改安全组规则或新建安全组。



### 查看关联安全组

您可参考如下步骤，查看引用参数模板的所有安全组实例。

1. 单击已创建的参数模板右侧的**查看关联**。



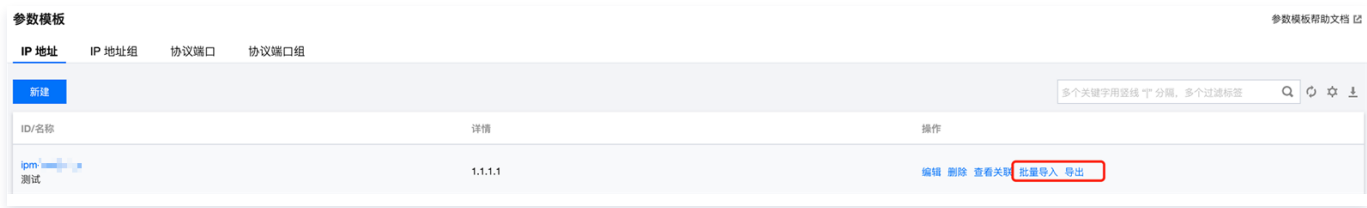
2. 在弹出的关联安全组列表中，将展示所有关联该参数模板的安全组实例。



### 导入参数模板

如需批量添加参数模板配置，可按照如下步骤操作。

1. 单击已创建的参数模板右侧的**批量导入**。



2. 上传本地文件。



### 导出参数模板

如需本地备份参数模板配置，可单击已创建的参数模板右侧的**导出**。





## 配置案例

最近更新时间：2023-12-19 16:50:21

### 参数模板使用案例

参数模板是安全组添加规则时一种高效、快捷、易维护的添加方式，例如当您需要添加多个地址段、指定 IP，及多个类型的协议端口时，可以定义参数模板，后期也可以通过参数模板来维护安全组规则中的 IP 来源和协议端口。

#### 说明

文中所有 IP 地址和协议端口均为举例，实际配置时，请根据业务实际情况进行替换。

### 示例描述

假设某用户期望配置如下安全组规则，且后续需要更新入站的来源 IP 范围和协议端口：

- 进站规则：
  - 允许来源 IP 范围：10.0.0.16-10.0.0.30，协议端口：TCP:80,443
  - 允许来源 CIDR 网段：192.168.3.0/24，协议端口：TCP:3600-15000
- 出站规则：  
拒绝目标 IP 地址：192.168.10.4，协议端口为：TCP:800

### 解决方案

由于用户多个 IP 网段和协议端口有相同的安全组策略，且后续需要更新来源 IP 范围，因此可结合参数模板来实现安全组规则的添加维护。

#### 步骤一：新建参数模板

1. 登录 [私有网络控制台](#)。
2. 选择左侧目录中的安全 > 参数模板，进入管理页面。
3. 在 IP 地址页签，单击新建，分别新建用于添加入站、出站规则的 IP 地址参数模板。
4. 在弹框中，输入来源 IP 地址范围，并单击确认。

### 新建 IP 地址

名称

IP 地址 <sup>①</sup>	备注	操作
<input type="text" value="1.1.1.1"/>	<input type="text" value="测试"/>	<span>✕</span>
<input type="text" value="请输入 IP 地址"/>	<input type="text"/>	<span>✕</span>

[+ 新增一行](#)

新建成功的 IP 地址参数模板如下图所示。

参数模板		参数模板帮助文档 <sup>①</sup>
ID/名称	详情	操作
<a href="#">ipm_...</a> 测试	1.1.1.1	<a href="#">编辑</a> <a href="#">删除</a> <a href="#">查看详情</a> <a href="#">批量导入</a> <a href="#">导出</a>

5. 在“协议端口”页签，单击新建，分别新建用于添加入站、出站规则的协议端口参数模板。

### 新建协议端口 ✕

名称

协议端口

协议端口	备注	操作
<input type="text" value="tcp:22"/>	<input type="text" value="ssh"/>	✕
<input type="text" value="tcp:80"/>	<input type="text" value="http"/>	✕

+ 新增一行

确定
取消

新建成功的协议端口参数模板如下图所示。

参数模板 参数模板帮助文档 [🔗](#)

IP 地址 IP 地址组 协议端口 协议端口组

新建 多个关键字用竖线“|”分隔，多个过滤标签  🔍 🔄 ⭐ ⬇

ID/名称	详情	操作
ppm- <span style="background-color: #ccc; padding: 2px;">[模糊]</span> 常见协议端口	tcp:22 <a href="#">查看全部</a>	编辑 删除 查看关联 批量导入 导出

## 步骤二：添加安全组规则

1. 登录 [私有网络控制台](#)。
2. 选择左侧目录中的安全 > 安全组，进入管理页面。
3. 在列表中，找到需要引用参数模板的安全组，单击其 ID，进入详情页。
4. 在入站规则/出站规则页签中，单击添加规则。
5. 在弹框中选择自定义类型，来源分类选择参数模板-IP地址/参数模板-IP地址组后，选中对应的IP地址/IP地址组，协议端口分别选择对应的协议端口参数模板，并单击确定。

### 添加入站规则 ✕

类型	来源 <span style="font-size: small;">①</span>	协议端口 <span style="font-size: small;">①</span>	策略	备注
自定义	参数模板 - IP 地址 测试(ipmi- <span style="background-color: #ccc; padding: 2px;">[模糊]</span> )	ppm- <span style="background-color: #ccc; padding: 2px;">[模糊]</span>	允许	

+ 新增一行

确定
取消

### 添加出站规则

类型	目标	协议端口	策略	备注
自定义	参数模板 - IP 地址 1111(ipm-0ge3ob8e)	ppm-4ty1ck3i	允许	

+新增一行

### 步骤三：更新参数模板

假设用户需要增加 IP 来源为10.0.1.0/27网段，协议端口为 UDP:58 的入站规则。可以直接更新 IP 地址 ipm-0ge3ob8e 和协议端口 ppm-4ty1ck3i 的参数模板。

1. 在参数模板的“IP 地址”页签，找到 ipm-0ge3ob8e 参数模板。
2. 在右侧单击编辑。

参数模板

IP 地址 IP 地址组 协议端口 协议端口组

新建

多个关键字用竖线“|”分隔，多个过滤标签

ID/名称	详情	操作
ipm-0ge3ob8e 测试	1.1.1.1	<a href="#">编辑</a> <a href="#">删除</a> <a href="#">查看关联</a> <a href="#">批量导入</a> <a href="#">导出</a>

3. 在弹框中，换行增加10.0.1.0/27网段，单击确定。

### 编辑 IP 地址

名称 测试

IP 地址	备注	操作
1.1.1.1	测试	✕
10.0.1.0/27		✕

+新增一行

4. 在参数模板的“协议端口”页签，找到 参数模板。
5. 在右侧单击编辑。

参数模板

IP 地址 IP 地址组 协议端口 协议端口组

新建

多个关键字用竖线“|”分隔，多个过滤标签

ID/名称	详情	操作
ppm-4ty1ck3i 常见协议端口	tcp:22 <a href="#">查看全部</a>	<a href="#">编辑</a> <a href="#">删除</a> <a href="#">查看关联</a> <a href="#">批量导入</a> <a href="#">导出</a>

6. 在弹框中，换行增加 UDP:58 入站协议端口，单击确定。

### 编辑协议端口 ✕

名称

协议端口

协议端口	备注	操作
<input type="text" value="tcp:22"/>	<input type="text" value="ssh"/>	<span>✕</span>
<input type="text" value="tcp:80"/>	<input type="text" value="http"/>	<span>✕</span>
<input type="text" value="udp:58"/>	<input type="text"/>	<span>✕</span>

[+ 新增一行](#)

# 访问管理

## 访问管理概述

最近更新时间：2023-10-12 15:54:41

如果您在腾讯云中使用了私有网络、云服务器、数据库等服务，这些服务由不同的人管理，但都共享您的云账号密钥，将存在如下问题：

- 您的密钥由多人共享，泄密风险高。
- 您无法限制其它人的访问权限，易产生误操作造成安全风险。

此时，您可以通过子账号实现不同的人管理不同的服务，来规避如上的问题。默认情况下，子账号没有使用 CVM 的权利或者 CVM 相关资源的权限。因此，我们就需要创建策略来允许子账号使用他们所需要的资源或权限。

### 说明

若您不需要对子账号进行 VPC 相关资源的访问管理，您可以跳过此章节，跳过这些部分不会影响您对文档中其余部分的理解和使用。

## 概述

**访问管理**（Cloud Access Management, CAM）可以帮助您安全、便捷地管理对腾讯云服务和服务资源的访问。您可以使用 CAM 创建子用户、用户组和角色，并通过策略控制其访问范围。CAM 支持用户和角色 SSO 能力，您可以根据具体管理场景针对性设置企业内用户和腾讯云的互通能力。

您最初创建的腾讯云主账号，拥有整个账号全部腾讯云服务和服务资源的完全访问权限，建议您保护好主账号的凭证信息，日常使用子用户或角色进行访问，并开启多因素校验和定时轮换密钥。

当您使用 CAM 的时候，可以将策略与一个用户或一组用户关联起来，策略能够授权或者拒绝用户使用指定资源完成指定任务。

- 有关 CAM 策略的更多相关基本信息，请参照 [语法逻辑](#)。
- 有关 CAM 策略的更多相关使用信息，请参照 [策略](#)。

## 入门

CAM 策略必须授权使用一个或多个 VPC 操作或者必须拒绝使用一个或多个 VPC 操作。同时还必须指定可以用于操作的资源（可以是全部资源，某些操作也可以是部分资源），策略还可以包含操作资源所设置的条件。

VPC 部分 API 操作不支持资源级权限，意味着，对于该类 API 操作，您不能在使用该类操作的时候指定某个具体的资源来使用，而必须要指定全部资源来使用。

任务	链接
了解策略基本结构	<a href="#">策略语法</a>
在策略中定义操作	<a href="#">VPC 的操作</a>
在策略中定义资源	<a href="#">VPC 的资源路径</a>
VPC 支持的资源级权限	<a href="#">VPC 支持的资源级权限</a>
控制台示例	<a href="#">控制台示例</a>

## 可授权的资源类型

最近更新时间：2023-08-01 17:40:52

### 策略语法

CAM 策略：

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

- 版本 **version** 是必填项，目前仅允许值为 "2.0"。
- 语句 **statement** 是用来描述一条或多条权限的详细信息。该元素包括 effect、action、resource、condition 等多个其他元素的权限或权限集合。一条策略有且仅有一个 statement 元素。
  1. **操作 action** 用来描述允许或拒绝的操作。操作可以是 API（以 name 前缀描述）或者功能集（一组特定的 API，以 permid 前缀描述）。该元素是必填项。
  2. **资源 resource** 描述授权的具体数据。资源是用六段式描述。每款产品的资源定义详情会有所区别。有关如何指定资源的信息，请参阅您编写的资源声明所对应的产品文档。该元素是必填项。
  3. **生效条件 condition** 描述策略生效的约束条件。条件包括操作符、操作键和操作值组成。条件值可包括时间、IP 地址等信息。有些服务允许您在条件中指定其他值。该元素是非必填项。
  4. **影响 effect** 描述声明产生的结果是允许还是显式拒绝。包括 allow（允许）和 deny（显式拒绝）两种情况。该元素是必填项。

### VPC 的操作

在 CAM 策略语句中，您可以从支持 CAM 的任何服务中指定任意的 API 操作。对于 VPC，请使用以 name/vpc: 为前缀的 API。例如：name/vpc:Describe 或者 name/vpc:CreateRoute。

如果您要在单个语句中指定多个操作的时候，请使用逗号将它们隔开，如下所示：

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

您也可以使用通配符指定多项操作。例如，您可以指定名字以单词 "Describe" 开头的所有操作，如下所示：

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

如果您要指定 VPC 中所有操作，请使用 \* 通配符，如下所示：

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

### VPC 的资源路径

每个 CAM 策略语句都有适用于自己的资源。

资源路径的一般形式如下：

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

- **project\_id**：描述项目信息，仅为了兼容 CAM 早期逻辑，无需填写。
- **service\_type**：产品简称，如 VPC。
- **region**：地域信息，如 bj。

- **account**: 资源拥有者的根账号信息, 如 uin/164256472。
- **resource**: 各产品的具体资源详情, 如 vpc/vpc\_id1 或者 vpc/\*。

例如, 您可以使用特定实例 (vpc-d08sl2zr) 在语句中指定它, 如下所示:

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

您还可以使用 \* 通配符指定属于特定账户的所有实例, 如下所示:

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

您要指定所有资源, 或者如果特定 API 操作不支持资源级权限, 请在 Resource 元素中使用 \* 通配符, 如下所示:

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

如果您想要在一条指令中同时指定多个资源, 请使用逗号将它们隔开, 如下所示为指定两个资源的例子:

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

下表描述了 VPC 能够使用的资源和对应的资源描述方法。

在下表中, \$ 为前缀的单词均为代称:

- 其中, project 指代的是项目 ID。
- 其中, region 指代的是地域。
- 其中, account 指代的是账户 ID。

资源	授权策略中的资源描述方法
VPC	qcs::vpc:\$region:\$account:vpc/\$vpcId
子网	qcs::vpc:\$region:\$account:subnet/\$subnetId
安全组	qcs::cvm:\$region:\$account:sg/\$sgId
EIP	qcs::cvm:\$region:\$account:eip/*

## VPC 访问管理策略示例

最近更新时间：2022-06-16 18:12:46

### VPC 的全读写策略

以下策略允许用户创建和管理 VPC。可向一组网络管理员关联此策略。Action 元素指定所有 VPC 相关 API。

```
{
  "version": "2.0",
  "statement": [
    {
      "action": [
        "name/vpc:*"
      ],
      "resource": "*",
      "effect": "allow"
    }
  ]
}
```

### VPC 的只读策略

以下策略允许用户查询您的 VPC 及相关资源。但用户无法创建、更新或删除它们。

在控制台，操作一个资源的前提是可以查看该资源，所以建议您为用户开通 VPC 只读权限。

```
{
  "version": "2.0",
  "statement": [
    {
      "action": [
        "name/vpc:Describe*",
        "name/vpc:Inquiry*",
        "name/vpc:Get*"
      ],
      "resource": "*",
      "effect": "allow"
    }
  ]
}
```

### 只允许子账号管理单个 VPC

以下策略允许用户看到所有 VPC，但只能操作 VPC A（假设 A 的 ID 是 vpc-d08sl2zr）及 A 下的网络资源（如子网、路由表等，不包括云服务器、数据库等），但不允许该用户管理其它 VPC。

该版本不支持只让用户看到 A，后续版本会支持。

```
{
  "version": "2.0",
  "statement": [
    {
      "action": "name/vpc:*",
      "resource": "*",
      "effect": "allow",
      "condition": {
        "string_equal_if_exist": { //请按照条件判断，只允许管理符合条件的VPC
          "vpc:vpc": [
            "vpc-d08sl2zr"
          ],
          "vpc:accepter_vpc": [
            "vpc-d08sl2zr"
          ],
        }
      }
    }
  ]
}
```



```

        "vpc:requester_vpc": [
          "vpc-d08sl2zr"
        ]
      }
    }
  }
}

```

## 允许用户管理 VPC，但不允许操作路由表

以下策略允许用户读写 VPC 及其相关资源，但是不允许用户对路由表进行相关操作。

```

{
  "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"
    }
  ]
}

```

## 允许用户管理 VPN 资源

该策略允许用户查看所有 VPC 资源，但只允许其对 VPN 进行增、删、改、查操作。

```

{
  "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"
    }
  ]
}

```

## VPC API 操作支持的资源级权限

最近更新时间：2024-03-13 17:02:41

在 CAM 中，可对私有网络资源进行以下 API 操作的授权，具体 API 支持的资源和条件的对应关系如下：

**注意:**

表中未列出的 VPC API 操作，即表示该 VPC API 操作不支持资源级权限。针对不支持资源级权限的 VPC API 操作，您仍可以向用户授予使用该操作的权限，但策略语句的资源元素必须指定为 \*。

API 操作	资源	条件	备注
AcceptVpcPeeringConnection	vpc 资源 qcs::vpc:\$region:\$account:vp c/*qcs::vpc:\$region:\$account: vpc/\$vpclId	vpc:region	vpc:region表示 vpc 所在地域。
—	对等连接资源 qcs::vpc:\$region:\$account:pc x/*qcs::vpc:\$region:\$account: pcx/\$peeringConnectionId	vpc:accepter_vpc vpc:regionvpc:reque ster_vpc	vpc:accepter_vpc 接收方 VPC，取值为接收方 VPC。 vpc:requester_vpc 表示发起方 VPC，取值为发起方 VPC。vpc:region 表示 vpc 所在地域。
—	vpc 资源 qcs::vpc:\$region:\$account:vp c/*qcs::vpc:\$region:\$account: vpc/\$vpclId(接收方 vpclId)	vpc:region	vpc:region 表示 vpc 所在地域。
AcceptVpcPeeringConnectionEx	对等连接资源 qcs::vpc:\$region:\$account:pc x/*qcs::vpc:\$region:\$account: pcx/\$peeringConnectionId	vpc:accepter_vpc vpc:accepter_vpc_r egionvpc:requester _vpcvpc:requester _vpc_region	vpc:accepter_vpc 接收方 VPC，取值为接收方 VPC。 vpc:accepter_vpc_region 表示接收方地域。 vpc:requester_vpc 表示发起方 VPC，取值为发起方 VPC。vpc:requester_vpc_region 表示发起方地域。
—	vpc 资源 qcs::vpc:\$region:\$account:vp c/*qcs::vpc:\$region:\$account: vpc/\$vpclId	vpc:region	vpc:region 表示 vpc 所在地域。
AddVpnConnEx	vpc 资源 qcs::vpc:\$region:\$account:vp c/*qcs::vpc:\$region:\$account: vpc/\$vpclId	vpc:region	vpc:region 表示 vpc 所在地域。
—	vpn 网关资源 qcs::vpc:\$region:\$account:vp ngw/*qcs::vpc:\$region:\$acco unt:vpngw/\$vpnGwId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地 域。
—	对端网关资源 qcs::vpc:\$region:\$account:cg w/*	vpc:region	vpc:region 表示 vpc 所在地域。
—	vpn 通道资源 qcs::vpc:\$region:\$account:vp nx/*	vpc:vpcvpc:vpngw vpc:region	vpc:vpc 表示开发商 VPC。vpc:vpngw 表示开发商下的 vpn 网关。vpc:region 表示 vpc 所在地域。
AssignPrivateIpAddresses	弹性网卡资源 qcs::vpc:\$region:\$account:eni /*qcs::vpc:\$region:\$account:e ni/\$networkInterfaceId	vpc:vpcvpc:subnet vpc:region	vpc:vpc 表示开发商的 VPC。vpc:subnet 表示开发商下的 子网。vpc:region 表示 vpc 所在地域。
AssociateRouteTable	子网资源 qcs::vpc:\$region:\$account:su bnet/*qcs::vpc:\$region:\$acco unt:subnet/\$subnetId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地 域。
—	路由表资源 qcs::vpc:\$region:\$account:rtb /*qcs::vpc:\$region:\$account:rt b/\$routeTableId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地 域。
AttachClassic	vpc 资源	vpc:region	vpc:region 表示 vpc 所在地域。

LinkVpc	qcs::vpc:\$region:\$account:vp c/*qcs::vpc:\$region:\$account: vpc/\$vpclD		
—	云服务器资源 qcs::cvm:\$region:\$account:in stance/*qcs::cvm:\$region:\$ac count:instance/\$instancelD	cvm:region	cvm:region 表示云服务器所在地域。
AttachNetwork Interface	弹性网卡资源 qcs::vpc:\$region:\$account:eni /*qcs::vpc:\$region:\$account:e ni/\$networkInterfacelD	vpc:vpcvpc:subnet vpc:region	vpc:vpc 表示开发者的 VPC。vpc:subnet 表示开发者下的子网。vpc:region 表示 vpc 所在地域。
—	云服务器资源 qcs::cvm:\$region:\$account:in stance/*qcs::cvm:\$region:\$ac count:instance/\$instancelD	cvm:region	cvm:region 表示云服务器所在地域。
CreateAndAtt achNetworkIn terface	vpc 资源 qcs::vpc:\$region:\$account:vp c/*qcs::vpc:\$region:\$account: vpc/\$vpclD	vpc:region	vpc:region 表示 vpc 所在地域。
—	云服务器资源 qcs::cvm:\$region:\$account:in stance/*qcs::cvm:\$region:\$ac count:instance/\$instancelD	cvm:region	cvm:region 表示云服务器所在地域。
—	弹性网卡资源 qcs::vpc:\$region:\$account:eni /*	vpc:vpcvpc:subnet vpc:region	vpc:vpc 表示开发者的 VPC。vpc:subnet 表示开发者下的子网vpc:region 表示 vpc 所在地域。
CreateDirectC onnectGatew ay	vpc 资源 qcs::vpc:\$region:\$account:vp c/*qcs::vpc:\$region:\$account: vpc/\$vpclD	vpc:region	vpc:region 表示 vpc 所在地域。
—	专线网关资源 qcs::vpc:\$region:\$account:dc g/*	vpc:vpcvpc:region	vpc:vpc 表示开发者 VPC。vpc:region 表示 vpc 所在地域。
CreateLocalD estinationIPP ortTranslationN atRule	专线网关资源 qcs::vpc:\$region:\$account:dc g/*qcs::vpc:\$region:\$account: d cg/\$directConnectGatewayId	vpc:vpcvpc:region	vpc:vpc 表示开发者 VPC。vpc:region 表示 vpc 所在地域。
CreateLocalIP TranslationAcl Rule	专线网关资源 qcs::vpc:\$region:\$account:dc g/*qcs::vpc:\$region:\$account: d cg/\$directConnectGatewayId	vpc:vpcvpc:region	vpc:vpc 表示开发者 VPC。vpc:region 表示 vpc 所在地域。
CreateLocalIP TranslationNa tRule	专线网关资源 qcs::vpc:\$region:\$account:dc g/*qcs::vpc:\$region:\$account: d cg/\$directConnectGatewayId	vpc:vpcvpc:region	vpc:vpc 表示开发者 VPC。vpc:region 表示 vpc 所在地域。
CreateLocalS ourceIPPortTr anslationAclR ule	专线网关资源 qcs::vpc:\$region:\$account:dc g/*qcs::vpc:\$region:\$account: d cg/\$directConnectGatewayId	vpc:vpcvpc:region	vpc:vpc 表示开发者 VPC。vpc:region 表示 vpc 所在地域。
CreateLocalS ourceIPPortTr anslationNatR ule	专线网关资源 qcs::vpc:\$region:\$account:dc g/*qcs::vpc:\$region:\$account: d cg/\$directConnectGatewayId	vpc:vpcvpc:region	vpc:vpc 表示开发者 VPC。vpc:region 表示 vpc 所在地域。
CreatePeerIP	专线网关资源	vpc:vpcvpc:region	vpc:vpc 表示开发者 VPC。vpc:region 表示 vpc 所在地

TranslationNatRule	qcs::vpc:\$region:\$account:dcg/*qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId		域。
CreateNatGateway	vpc 资源 qcs::vpc:\$region:\$account:vpc/*qcs::vpc:\$region:\$account:vpc/\$vpcId	vpc:region	vpc:region 表示 vpc 所在地域。
—	nat 网关资源 qcs::vpc:\$region:\$account:nat/*	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
CreateNetworkAcl	vpc 资源 qcs::vpc:\$region:\$account:vpc/*qcs::vpc:\$region:\$account:vpc/\$vpcId	vpc:region	vpc:region 表示 vpc 所在地域。
—	网络 acl 资源 qcs::vpc:\$region:\$account:acl/*	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
CreateNetworkInterface	vpc 资源 qcs::vpc:\$region:\$account:vpc/*qcs::vpc:\$region:\$account:vpc/\$vpcId	vpc:region	vpc:region 表示 vpc 所在地域。
—	子网资源 qcs::vpc:\$region:\$account:subnet/*qcs::vpc:\$region:\$account:subnet/\$subnetId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
—	弹性网卡资源 qcs::vpc:\$region:\$account:eni/*	vpc:vpcvpc:subnet vpc:region	vpc:vpc 表示开发商 VPC。vpc:subnet 表示开发商子网 vpc:region 表示 vpc 所在地域。
CreateRoute	路由表资源 qcs::vpc:\$region:\$account:rtb/*qcs::vpc:\$region:\$account:rtb/\$routeTableId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
CreateRouteTable	vpc 资源 qcs::vpc:\$region:\$account:vpc/*qcs::vpc:\$region:\$account:vpc/\$vpcId	vpc:region	vpc:region 表示 vpc 所在地域。
—	路由表资源 qcs::vpc:\$region:\$account:rtb/*	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
CreateSubnet	vpc 资源 qcs::vpc:\$region:\$account:vpc/*qcs::vpc:\$region:\$account:vpc/\$vpcId	vpc:region	vpc:region 表示 vpc 所在地域。
—	子网网关资源 qcs::vpc:\$region:\$account:subnet/*	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
CreateSubnetAclRule	网络 acl 资源 qcs::vpc:\$region:\$account:acl/*qcs::vpc:\$region:\$account:acl/\$networkAclId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
—	子网网关资源 qcs::vpc:\$region:\$account:subnet/*	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。

CreateVpcPeeringConnection	vpc 资源(发起方)qcs::vpc:\$region:\$account:vpc/*qcs::vpc:\$region:\$account:vpc/\$vpcId	vpc:region	vpc:region 表示 vpc 所在地域。
—	对等连接资源 qcs::vpc:\$region:\$account:pcx/*	vpc:accepter_vpcvpc:requester_vpcvpc:region	vpc:accepter_vpc 接收方 VPC, 取值为接收方 VPC。 vpc:requester_vpc 表示发起方 VPC, 取值为发起方 VPC。 vpc:region 表示 vpc 所在地域。
CreateVpcPeeringConnectionEx	vpc 资源 qcs::vpc:\$region:\$account:vpc/*qcs::vpc:\$region:\$account:vpc/\$vpcId	vpc:region	vpc:region 表示 vpc 所在地域。
—	对等连接资源 qcs::vpc:\$region:\$account:pcx/*	vpc:accepter_vpcvpc:accepter_vpc_regionvpc:requester_vpcvpc:requester_vpc_region	vpc:accepter_vpc 接收方 VPC, 取值为接收方 VPC。 vpc:accepter_vpc_region 表示接收方地域。 vpc:requester_vpc 表示发起方 VPC, 取值为发起方 VPC。 vpc:requester_vpc_region 表示发起方地域。
DeleteDirectConnectGateway	专线网关资源 qcs::vpc:\$region:\$account:dcg/*qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
DeleteLocalDestinationPortTranslationNatRule	专线网关资源 qcs::vpc:\$region:\$account:dcg/*qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
DeleteLocalIPTranslationAclRule	专线网关资源 qcs::vpc:\$region:\$account:dcg/*qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
DeleteLocalIPTranslationNatRule	专线网关资源 qcs::vpc:\$region:\$account:dcg/*qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
DeleteLocalSourceIPPortTranslationAclRule	专线网关资源 qcs::vpc:\$region:\$account:dcg/*qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
DeletePeerIPTranslationNatRule	专线网关资源 qcs::vpc:\$region:\$account:dcg/*qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
DeleteLocalSourceIPPortTranslationNatRule	专线网关资源 qcs::vpc:\$region:\$account:dcg/*qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
DeleteNatGateway	nat 网关资源 qcs::vpc:\$region:\$account:nat/*qcs::vpc:\$region:\$account:nat/\$natId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
DeleteNetworkAcl	网络 acl 资源 qcs::vpc:\$region:\$account:acl/*qcs::vpc:\$region:\$account:acl/\$networkAclId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
DeleteNetworkInterface	弹性网卡资源 qcs::vpc:\$region:\$account:eni	vpc:vpcvpc:subnetvpc:region	vpc:vpc 表示开发商的 VPC。vpc:subnet 表示开发商下的子网。vpc:region 表示 vpc 所在地域。

	/*qcs::vpc:\$region:\$account:eni/\$networkInterfaceId		
DeleteRoute	路由表资源 qcs::vpc:\$region:\$account:rtb/*qcs::vpc:\$region:\$account:rtb/\$routeTableId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
DeleteRouteTable	路由表资源 qcs::vpc:\$region:\$account:rtb/*qcs::vpc:\$region:\$account:rtb/\$routeTableId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
DeleteSubnet	子网资源 qcs::vpc:\$region:\$account:subnet/*qcs::vpc:\$region:\$account:subnet/\$subnetId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
DeleteUserGw	对端网关资源 qcs::vpc:\$region:\$account:cgw/*qcs::vpc:\$region:\$account:cgw/\$userGwId	vpc:region	vpc:region 表示 vpc 所在地域。
DeleteVpc	vpc 资源 qcs::vpc:\$region:\$account:vpc/*qcs::vpc:\$region:\$account:vpc/\$vpcId	vpc:regionvpc:vpc	vpc:region 表示 vpc 所在地域。
DeleteVpcPeeringConnection	对等连接资源 qcs::vpc:\$region:\$account:pcx/*qcs::vpc:\$region:\$account:pcx/\$peeringConnectionId	vpc:accepter_vpcvpc:regionvpc:requester_vpc	vpc:accepter_vpc 接收方 VPC，取值为接收方 VPC。vpc:requester_vpc 表示发起方 VPC，取值为发起方 VPC。vpc:region 表示 vpc 所在地域。
DeleteVpcPeeringConnectionEx	对等连接资源 qcs::vpc:\$region:\$account:pcx/*qcs::vpc:\$region:\$account:pcx/\$peeringConnectionId	vpc:accepter_vpcvpc:accepter_vpc_regionvpc:requester_vpcvpc:requester_vpc_region	vpc:accepter_vpc 接收方 VPC，取值为接收方 VPC。vpc:accepter_vpc_region 表示接收方地域。vpc:requester_vpc 表示发起方 VPC，取值为发起方 VPC。vpc:requester_vpc_region 表示发起方地域。
DeleteVpnConn	vpn 通道资源 qcs::vpc:\$region:\$account:vpn/*qcs::vpc:\$region:\$account:vpn/\$vpnConnId	vpc:vpcvpc:vpngwvpc:usergwvpc:region	vpc:vpc 表示开发商的 VPC。vpc:vpngw 表示开发商下的网关。vpc:usergw 表示开发商下的对端网关。vpc:region 表示 vpc 所在地域。
DetachClassicLinkVpc	vpc 资源 qcs::vpc:\$region:\$account:vpc/*qcs::vpc:\$region:\$account:vpc/\$vpcId	vpc:regionvpc:vpc	vpc:region 表示 vpc 所在地域。
—	云服务器资源 qcs::cvm:\$region:\$account:instance/*qcs::cvm:\$region:\$account:instance/\$instanceId	cvm:region	cvm:region 表示云服务器所在地域。
DetachNetworkInterface	云服务器资源 qcs::cvm:\$region:\$account:instance/*qcs::cvm:\$region:\$account:instance/\$instanceId	cvm:region	cvm:region 表示云服务器所在地域。
—	弹性网卡资源 qcs::vpc:\$region:\$account:eni/*qcs::vpc:\$region:\$account:eni/\$networkInterfaceId	vpc:vpcvpc:subnetvpc:region	vpc:vpc 表示开发商的 VPC。vpc:subnet 表示开发商下的子网。vpc:region 表示 vpc 所在地域。
DeteteSubnetAclRule	子网资源 qcs::vpc:\$region:\$account:subnet/*qcs::vpc:\$region:\$account:subnet/\$subnetId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。

—	网络 acl 资源 qcs::vpc:\$region:\$account:acl/*qcs::vpc:\$region:\$account:acl/\$networkAclId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
EipBindNatGateway	nat 网关资源 qcs::vpc:\$region:\$account:nat/*qcs::vpc:\$region:\$account:nat/\$natId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
EipUnBindNatGateway	nat 网关资源 qcs::vpc:\$region:\$account:nat/*qcs::vpc:\$region:\$account:nat/\$natId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
EnableVpcPeeringConnection	vpc 资源 qcs::vpc:\$region:\$account:vpc/*qcs::vpc:\$region:\$account:vpc/\$vpcId	vpc:region	vpc:region 表示 vpc 所在地域。
—	对等连接资源 qcs::vpc:\$region:\$account:pcx/*qcs::vpc:\$region:\$account:pcx/\$peeringConnectionId	vpc:accepter_vpcvpc:regionvpc:requester_vpc	vpc:accepter_vpc 接收方 VPC，取值为接收方 VPC。vpc:requester_vpc 表示发起方 VPC，取值为发起方 VPC。vpc:region 表示 vpc 所在地域。
EnableVpcPeeringConnectionEx	vpc 资源 qcs::vpc:\$region:\$account:vpc/*qcs::vpc:\$region:\$account:vpc/\$vpcId	vpc:region	vpc:region 表示 vpc 所在地域。
—	对等连接资源 qcs::vpc:\$region:\$account:pcx/*qcs::vpc:\$region:\$account:pcx/\$peeringConnectionId	vpc:accepter_vpcvpc:accepter_vpc_regionvpc:requester_vpcvpc:requester_vpc_region	vpc:accepter_vpc 接收方 VPC，取值为接收方 VPC。vpc:accepter_vpc_region 表示接收方地域。vpc:requester_vpc 表示发起方 VPC，取值为发起方 VPC。vpc:requester_vpc_region 表示发起方地域。
MigrateNetworkInterface	弹性网卡资源 qcs::vpc:\$region:\$account:eni/*qcs::vpc:\$region:\$account:eni/\$networkInterfaceId	vpc:vpcvpc:subnetvpc:region	vpc:vpc 表示开发商的 VPC。vpc:subnet 表示开发商下的子网。vpc:region 表示 vpc 所在地域。
—	云服务器资源 qcs::cvm:\$region:\$account:instance/*qcs::cvm:\$region:\$account:instance/\$instanceId(迁移前后的都需要授权)	cvm:region	cvm:region 表示云服务器所在地域。
MigratePrivateIpAddress	弹性网卡资源 qcs::vpc:\$region:\$account:eni/*qcs::vpc:\$region:\$account:eni/\$networkInterfaceId	vpc:vpcvpc:subnetvpc:region	vpc:vpc 表示开发商的 VPC。vpc:subnet 表示开发商下的子网。vpc:region 表示 vpc 所在地域。
ModifyDirectConnectGateway	专线网关资源 qcs::vpc:\$region:\$account:dcdg/*qcs::vpc:\$region:\$account:dcdg/\$directConnectGatewayId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
ModifyLocalDestinationIPPortTranslationNatRule	专线网关资源 qcs::vpc:\$region:\$account:dcdg/*qcs::vpc:\$region:\$account:dcdg/\$directConnectGatewayId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
ModifyLocalIPTranslationAclRule	专线网关资源 qcs::vpc:\$region:\$account:dcdg/*qcs::vpc:\$region:\$account:dcdg/\$directConnectGatewayId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。



ModifyLocalIPTranslationNatRule	专线网关资源 qcs::vpc:\$region:\$account:dcg/*qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
ModifyLocalSourceIPPortTranslationACLRule	专线网关资源 qcs::vpc:\$region:\$account:dcg/*qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
ModifyPeerIPTranslationNatRule	专线网关资源 qcs::vpc:\$region:\$account:dcg/*qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
ModifyLocalSourceIPPortTranslationNatRule	专线网关资源 qcs::vpc:\$region:\$account:dcg/*qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
ModifyNatGateway	nat 网关资源 qcs::vpc:\$region:\$account:nat/*qcs::vpc:\$region:\$account:nat/nat-dc7cdf	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
ModifyNetworkACL	网络 acl 资源 qcs::vpc:\$region:\$account:acl/*qcs::vpc:\$region:\$account:acl/\$networkACLId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
ModifyNetworkACLEntry	网络 acl 资源 qcs::vpc:\$region:\$account:acl/*qcs::vpc:\$region:\$account:acl/\$networkACLId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
ModifyNetworkInterface	弹性网卡资源 qcs::vpc:\$region:\$account:eni/*qcs::vpc:\$region:\$account:eni/\$networkInterfaceId	vpc:vpcvpc:subnet vpc:region	vpc:vpc 表示开发商的 VPC。vpc:subnet 表示开发商下的子网。vpc:region 表示 vpc 所在地域。
ModifyPrivateIPAddress	弹性网卡资源 qcs::vpc:\$region:\$account:eni/*qcs::vpc:\$region:\$account:eni/\$networkInterfaceId	vpc:vpcvpc:subnet vpc:region	vpc:vpc 表示开发商的 VPC。vpc:subnet 表示开发商下的子网。vpc:region 表示 vpc 所在地域。
ModifyRouteTableAttribute	路由表资源 qcs::vpc:\$region:\$account:rtb/*qcs::vpc:\$region:\$account:rtb/\$routeTableId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
ModifySubnetAttribute	子网资源 qcs::vpc:\$region:\$account:subnet/*qcs::vpc:\$region:\$account:subnet/\$subnetId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
ModifyUserGateway	对端网关资源 qcs::vpc:\$region:\$account:cgw/*qcs::vpc:\$region:\$account:cgw/\$userGatewayId	vpc:region	vpc:region 表示 vpc 所在地域。
ModifyVpcAttribute	vpc 资源 qcs::vpc:\$region:\$account:vpc/*qcs::vpc:\$region:\$account:vpc/\$vpcId	vpc:Region	vpc:region 表示 vpc 所在地域。
ModifyVpcPeeringConnection	vpc 资源 qcs::vpc:\$region:\$account:vpc	vpc:region	vpc:region 表示 vpc 所在地域。

	c/*qcs::vpc:\$region:\$account:vpc/\$vpclId		
—	对等连接资源 qcs::vpc:\$region:\$account:pcx/*qcs::vpc:\$region:\$account:pcx/\$peeringConnectionId	vpc:accepter_vpcvpc:regionvpc:requester_vpc	vpc:accepter_vpc 接收方 VPC，取值为接收方 VPC。vpc:requester_vpc 表示发起方 VPC，取值为发起方 VPC。vpc:region 表示 vpc 所在地域。
ModifyVpcPeeringConnectionEx	vpc 资源 qcs::vpc:\$region:\$account:vpc/*qcs::vpc:\$region:\$account:vpc/\$vpclId	vpc:region	vpc:region 表示 vpc 所在地域。
—	对等连接资源 qcs::vpc:\$region:\$account:pcx/*qcs::vpc:\$region:\$account:pcx/\$peeringConnectionId	vpc:accepter_vpcvpc:accepter_vpc_regionvpc:requester_vpcvpc:requester_vpc_region	vpc:accepter_vpc 接收方 VPC，取值为接收方 VPC。vpc:accepter_vpc_region 表示接收方地域。vpc:requester_vpc 表示发起方 VPC，取值为发起方 VPC。vpc:requester_vpc_region 表示发起方地域。
ModifyVpnConnEx	vpn 通道资源 qcs::vpc:\$region:\$account:vpn/*qcs::vpc:\$region:\$account:vpn/\$vpnConnId	vpc:vpcvpc:vpngwvpc:usergwvpc:region	vpc:vpc 表示开发商的 VPC。vpc:vpngw 表示开发商下的网关。vpc:usergw 表示开发商下的对端网关。vpc:region 表示 vpc 所在地域。
ModifyVpnGw	vpn 网关资源 qcs::vpc:\$region:\$account:vpngw/*qcs::vpc:\$region:\$account:vpngw/\$vpnGwId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
RejectVpcPeeringConnection	vpc 资源 qcs::vpc:\$region:\$account:vpc/*qcs::vpc:\$region:\$account:vpc/\$vpclId	vpc:region	vpc:region 表示 vpc 所在地域。
—	对等连接资源 qcs::vpc:\$region:\$account:pcx/*qcs::vpc:\$region:\$account:pcx/\$peeringConnectionId	vpc:accepter_vpcvpc:regionvpc:requester_vpc	vpc:accepter_vpc 接收方 VPC，取值为接收方 VPC。vpc:requester_vpc 表示发起方 VPC，取值为发起方 VPC。vpc:region 表示 vpc 所在地域。
RejectVpcPeeringConnectionEx	vpc 资源 qcs::vpc:\$region:\$account:vpc/*qcs::vpc:\$region:\$account:vpc/\$vpclId	vpc:region	vpc:region 表示 vpc 所在地域。
—	对等连接资源 qcs::vpc:\$region:\$account:pcx/*qcs::vpc:\$region:\$account:pcx/\$peeringConnectionId	vpc:accepter_vpcvpc:accepter_vpc_regionvpc:requester_vpcvpc:requester_vpc_region	vpc:accepter_vpc 接收方 VPC，取值为接收方 VPC。vpc:accepter_vpc_region 表示接收方地域。vpc:requester_vpc 表示发起方 VPC，取值为发起方 VPC。vpc:requester_vpc_region 表示发起方地域。
ResetVpnConnSA	vpn 通道资源 qcs::vpc:\$region:\$account:vpn/*qcs::vpc:\$region:\$account:vpn/\$vpnConnId	vpc:vpcvpc:vpngwvpc:usergwvpc:region	vpc:vpc 表示开发商的 VPC。vpc:vpngw 表示开发商下的网关。vpc:usergw 表示开发商下的对端网关。vpc:region 表示 vpc 所在地域。
SetLocalIPTranslationACLRule	专线网关资源 qcs::vpc:\$region:\$account:dcg/*qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
SetLocalSourceIPPortTranslationACLRule	专线网关资源 qcs::vpc:\$region:\$account:dcg/*qcs::vpc:\$region:\$account:dcg/\$directConnectGatewayId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。
SetSSLVpnDomain	vpn 网关资源 qcs::vpc:\$region:\$account:vpngw/*qcs::vpc:\$region:\$account:vpngw/\$vpnGwId	vpc:vpcvpc:region	vpc:vpc 表示开发商 VPC。vpc:region 表示 vpc 所在地域。

	ngw/*qcs::vpc:\$region:\$account:vpngw/\$vpnGwId		
UnassignPrivateIpAddresses	弹性网卡资源 qcs::vpc:\$region:\$account:eni/*qcs::vpc:\$region:\$account:eni/\$networkInterfaceId	vpc:vpcvpc:subnet vpc:region	vpc:vpc 表示开发商的 VPC。vpc:subnet 表示开发商下的子网。vpc:region 表示 vpc 所在地域。

# 诊断工具

## 网络探测

最近更新时间：2023-10-27 14:27:34

腾讯云网络探测是监控 VPC 网络连接质量的服务，可为您监控网络连接的时延、丢包率等关键指标。

在混合云网络架构下，您将使用 VPN/专线/云联网连接云上 VPC 和您的自有 IDC，为了实时监控连接的网络质量，您可以在需要与 IDC 通信的子网内创建网络探测对象，探测对象创建后将返回探测的链路的丢包率及时延，帮助您实现如下功能：

- 连接质量实时监控。
- 连接故障实时告警。

### 使用说明

- 网络探测为 Ping 探测，频率：20次/分钟。
- 每个私有网络内最多可创建50个网络探测实例。
- 同一个 VPC 下最多20个子网可以创建网络探测。

### 创建网络探测

1. 登录 [私有网络控制台](#)。
2. 在左侧目录中，选择**诊断工具** > **网络探测**。
3. 在管理页面上方单击**新建**。
4. 在“新建网络探测”弹窗中，填写相关字段。

#### 说明

- 网络探测路由为系统路由，不可修改。
- 在子网切换路由时，原子网关路由表将删除此系统路由，子网新关联的路由表将添加此系统路由。

新建网络探测
×

名称

私有网络

子网  ⓘ

探测目的IP  验证 ⓘ

验证

源端下一跳路由  不指定  指定 ⓘ

NAT网关  ⓘ

统计方式 平均值

备注

字段说明：

字段	含义
名称	网络探测名称。
私有网络	探测源 IP 所在的私有网络。
子网	探测源 IP 所在的子网。
探测目的 IP	网络探测最大支持两个目的 IP 地址，请为网络探测的目的主机开通 ICMP 防火墙策略。
源端下一跳路由	<p>可选择<b>不指定</b>和<b>指定</b>。</p> <ul style="list-style-type: none"> <li>若选择<b>不指定</b>，则默认不选择下一跳路由，使用已有 VPC 路由表转发。</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <p><b>说明：</b> 不指定源端下一跳路由为白名单功能，如需使用请 <a href="#">在线咨询</a> 进行申请。</p> </div> <ul style="list-style-type: none"> <li>若选择<b>指定</b>，则需选择下一跳类型和具体实例，配置下一跳对象后，系统将自动在子网所关联的路由表中添加对应的32位路由。目前支持的源端下一跳网关类型有：NAT 网关、对等连接、VPN 网关、专线网关、云服务器（公网网关）、云服务器、云联网。</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <p><b>说明：</b> 如果下一跳指定为云联网，当探测目的 IP 同时存在于云联网中两个 VPC 时，按照最长掩码匹配，即网段掩码大的路由生效。</p> </div>

5. (可选) 字段填写完成后，在“探测目的 IP”后，单击**验证**。

**说明**

本步骤仅适用于**指定**源端下一跳路由，**不指定**请跳过。

- 若连接成功，单击**确定**即可。
- 若连接失败，请检查子网路由是否配置正确或目的探测对象是否放通了网络 ACL、安全组等防火墙，详情请参见 [管理网络 ACL](#) 及 [修改安全组规则](#)。

## 查看网络探测时延和丢包率

- 登录 [私有网络控制台](#)。
- 在左侧目录中，选择**诊断工具 > 网络探测**。
- 在目标网络探测实例的“监控”列，单击 ，即可查看网络探测时延及丢包率。



## 修改网络探测

- 登录 [私有网络控制台](#)。
- 在左侧目录中，选择**诊断工具 > 网络探测**。
- 在网络探测实例列表中，找到需要修改的网络探测实例，在右侧操作列，单击**编辑**。

ID/名称	状态	监控	私有网络	子网	源IP	下一跳	探测目的IP	备注	操作
netd- ee	运行中		vpc- pen	sub- per	10. 10.	未指定	220.	-	<a href="#">编辑</a> <a href="#">删除</a>

4. 在编辑网络探测对话框中，输入需要修改的信息，并单击**确定**。

**说明**

- 本例以**不指定源端下一跳路由**实例为例。
- **不指定源端下一跳路由**支持修改：名称、探测目的 IP、备注。
- **指定源端下一跳**支持修改：名称、探测目的 IP、源端下一跳路由、备注。

**编辑网络探测**

名称

私有网络

子网

探测目的IP  验证

选填 验证

统计方式 平均值

备注

### 删除网络探测

1. 登录 [私有网络控制台](#)。
2. 在左侧目录中，选择**诊断工具 > 网络探测**。
3. 在网络探测实例列表中，找到需要删除的网络探测实例，在右侧操作列，单击**删除**。
4. 在弹出的确认框中，单击**删除**即可。

**注意**

删除网络探测实例，将一并删除关联告警策略、网络探测的路由配置，请评估业务影响后谨慎操作。

ID/名称	状态	监控	私有网络	子网	源IP	下一跳	探测目的IP	备注	操作
netd- ee-	运行中		vpc- pen-	subn- pen-	10. 10.	未指定	220.	-	编辑 <b>删除</b>

### 配置告警

可以为网络探测配置监控告警，当探测到路由异常时，可以及时告警到用户，以便快速进行路由切换，保障业务可用性。

1. 登录 [告警策略控制台](#)。
2. 单击**新建**，在弹出的新建告警策略对话框中，填写策略名称，设置策略类型为**私有网络 / 网络探测**，选择具体实例，配置告警触发条件及告警通知等信息，单击**完成**即可。

## 实例端口验通

最近更新时间：2023-10-27 14:27:35

实例端口验通功能可以帮助您检测云服务器实例的安全组端口放行情况，定位故障所在，提升使用体验。本功能提供常用端口和自定义端口的检测，常用端口如下表所示。

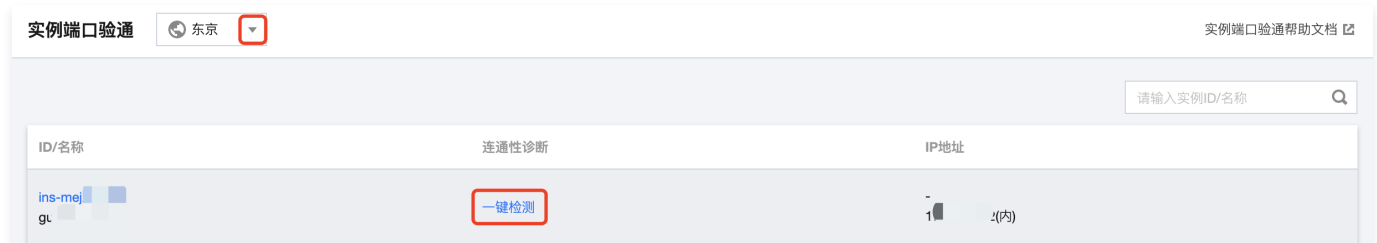
规则类型	端口	说明
入站规则	ICMP 协议	用于传递控制消息，如 ping 命令。ICMP 为控制协议，不涉及端口号。
	TCP:20	用于放行 FTP 服务的上传、下载。
	TCP:21	
	TCP:22	用于放行 Linux SSH 登录。
	TCP:3389	用于放行 Windows 远程登录。
	TCP:443	用于提供网站 HTTPS 服务。
	TCP:80	用于提供网站 HTTP 服务。
出站规则	ALL	用于放行所有出站流量，以访问外部网络。

### 前提条件

已创建云服务器实例，请参见 [实例创建指引](#)。

### 操作指南

1. 登录 [私有网络控制台](#)。
2. 单击左侧目录下方的 **诊断工具** > **实例端口验通**，进入管理页面。
3. 在页面上方选择 **地域**，并在列表中，找到您要验证的实例所在行，单击 **一键检测**。



4. 您可以在弹窗中看到端口验通的详情，请根据实际情况选择执行如下操作。
  - 如不需要检测常用端口，可以取消勾选该条检测条目。
  - 如常用端口不满足检测要求，可在下方的自定义端口中输入需要检测的端口号，并单击 **保存**。
    - 协议：可选择 TCP 或 UDP。
    - 端口：输入需要验通的端口号，注意，端口号不可与常用端口号重复。
    - 方向：可选择入站或者出站。
    - IP：当方向为入站时，请填写输入源IP；当方向为出站时，请填写目的IP；所有来源或目的地址，请填写 ALL。
    - 自定义端口检测最多支持15个。

例如，除检测常用端口外，还需要自定义检测 TCP 协议、30端口，出站方向，目的 IP 为10.0.1.12的安全策略，可在自定义端口检测区域框中输入如下图所示的信息。

端口检测

<input checked="" type="checkbox"/> 协议	端口	方向	策略	影响
<input checked="" type="checkbox"/> ICMP	-	入站	放通	无
<input checked="" type="checkbox"/> TCP	20	入站	放通	无
<input checked="" type="checkbox"/> TCP	21	入站	放通	无
<input checked="" type="checkbox"/> TCP	22	入站	放通	无
<input checked="" type="checkbox"/> TCP	3389	入站	放通	无
<input checked="" type="checkbox"/> TCP	443	入站	放通	无
<input checked="" type="checkbox"/> TCP	80	入站	放通	无
<input checked="" type="checkbox"/> ALL	ALL	出站	放通	无

常用端口

自定义端口检测

协议	端口	方向	IP ⓘ	策略	操作
TCP	30	出站	10.0.1.12	放通	删除

你还可以添加14个

自定义端口

开始检测

5. 完成端口检查设置后，单击开始检测，策略列将展示检测结果。

自定义端口检测

协议	端口	方向	IP ⓘ	策略	操作
TCP	30	出站	10.0.1.12	放通	删除

你还可以添加14个

开始检测

如果您存在某条端口策略为未放通，且有放通该端口的需求（例如 TCP:22），如下图所示。



<input checked="" type="checkbox"/> TCP	22	入站	未放通	无法使用ssh功能
---	----	----	-----	-----------

那么，您可以在 [安全组控制台](#) 进入实例绑定的安全组，添加一条放通 TCP:22 端口的入站规则，可根据实际需求，在来源中默认选择 all 放通全部 IP，或填写指定 IP（IP 段），如下图所示。

### 添加入站规则

类型	来源 <sup>①</sup>	协议端口 <sup>①</sup>	策略	备注
Linux登录(22)	all	TCP:22	允许	放通Linux SSH登录

[+新增一行](#)

## 相关信息

- 如需了解安全组相关内容，请参见 [安全组概述](#)、[添加安全组规则](#)。
- 如需了解服务器常用端口相关说明，请参见 [服务器常用端口](#)。

# 网关流控

最近更新时间：2023-10-27 14:27:35

网关流控可以为您提供网关上 IP 粒度的“监”与“控”能力，可以对内网 IP 与网关之间的带宽进行监控和限制。

开启网关流控可使流量管理精细化、可视化，帮助网络运维人员掌握网关中流量的情况，IP 粒度的限速能力帮助您快速排查故障，屏蔽异常流量，保障关键业务。

目前支持开启网关流控的有：[NAT 网关](#)、[VPN 连接](#)、[对等连接](#)、[专线网关](#)。

## 说明

1. 黑石侧对等连接、云联网暂不支持开启网关流控。
2. 网关流控的源端仅支持云服务器，其它服务到网关的流量不支持统计。
3. 目前网关流控处于灰度中，如有需要，请提交 [工单申请](#)。

## 主要功能

- 精确的网关故障排查能力，最小化网络故障时间；可以结合流量提供实时查询、展示 TOP N 排名的 IP 功能，分析来源 IP 及其关键指标，快速定位异常流量。
- 基于 IP - 网关粒度的“监”与“控”能力；结合分钟级的网络流量查询，可及时发现异常流量抢占带宽，设置 IP - 网关粒度带宽限制，保障核心业务稳定畅行。
- 全时全流的网关流量分析能力，降低云上网络成本。通过 QoS 控制成本，可在网络预算有限的情况下，限制非关键业务带宽，以降低成本。

## 应用场景

主要应用于公司网关流量在夜间突增场景，通过智能网关流控，运维人员可根据该突增时间点，追踪造成流量突增的 IP，从而快速定位根源。不仅如此，网关流控提供基于 IP - 网关粒度的带宽控制，可限制某 IP 到网关的带宽，屏蔽异常流量，保障关键业务。

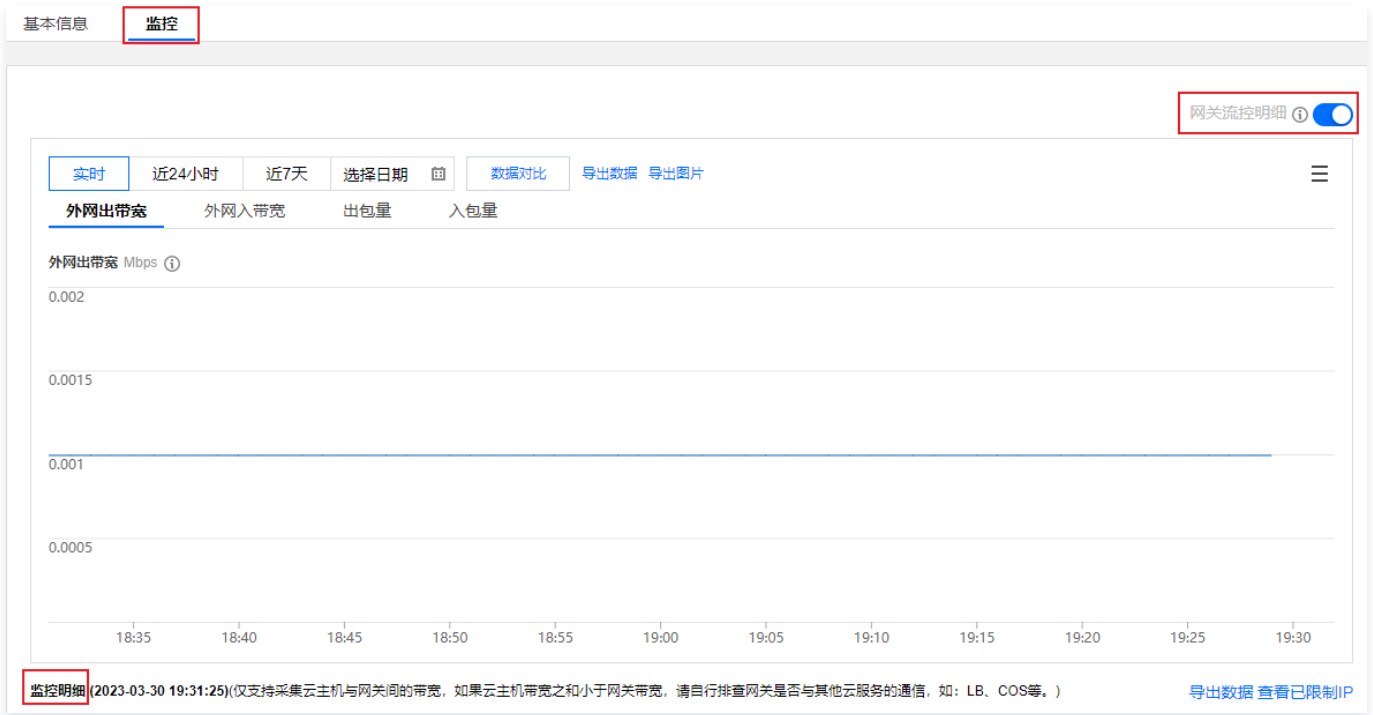
## 计费相关

网关流控功能不收费。

## 操作指南

### 开启网关流控明细

1. 登录 [私有网络控制台](#)。
2. 根据您的需求，在左侧导航栏选择 [NAT 网关](#)、[VPN 连接](#) > [VPN 网关](#)、[对等连接](#)或[专线网关](#)，进入对应管理页面，如下以 [VPN 网关](#) 为例。
3. 单击需要开启的网关或连接 ID，进入详情页。
4. 单击[监控](#)选项卡，开启右上角[网关流控明细](#)。
5. 开启 [VPN 网关流控](#)明细需要 5 - 6 分钟采集和发布数据，之后，您即可在监控图表下方查看监控明细表格。



### 设置流控明细

1. 登录 [私有网络控制台](#)。
2. 根据您的需求，在左侧导航栏选择 **NAT 网关**、**VPN 连接** > **VPN 网关**、**对等连接**或**专线网关**，进入对应管理页面，如下以 VPN 网关为例。
3. 单击需要设置的网关或连接 ID，进入详情页。
4. 单击**监控**选项卡。
5. 找到需要限制出带宽上限的 IP，单击**修改**。

IP地址	云服务器ID	云服务器名称	出带宽(Mbps)	入带宽(Mbps)	出带宽上限(Mbps)
1	i	windows	0.00	0.00	无限制 <span>修改</span>

6. 调整带宽后，单击**保存**。

IP地址	云服务器ID	云服务器名称	出带宽(Mbps)	入带宽(Mbps)	出带宽上限(Mbps)
1	i	windows	0.00	0.00	无限制

III  Mbps

提示：IP的绑定关系发生变更时（如云服务器销毁，更换内网IP），带宽限制将会失效

保存 取消

### 查看流控明细

1. 登录 [私有网络控制台](#)。
2. 根据您的需求，在左侧导航栏选择 **NAT 网关**、**VPN 连接** > **VPN 网关**、**对等连接**或**专线网关**，进入对应管理页面，如下以 VPN 网关为例。
3. 单击需要查看的网关或连接 ID，进入详情页。
4. 单击**监控**选项卡。
5. 在网关流控明细表右上方，单击**查看已限制 IP**。

监控明细 (2019-11-14 18:21:42)

[查看已限制IP](#)

IP地址	云服务器ID <sup>①</sup>	云服务器名称	出带宽(Mbps) <sup>⬆</sup>	入带宽(Mbps) <sup>⬆</sup>	出带宽上限(Mbps)
------	---------------------	--------	------------------------	------------------------	-------------

6. 流控明细如下图所示。

IP地址	云服务器ID <sup>①</sup>	云服务器名称	出带宽上限(Mbps) <sup>⬆</sup>	操作
1	i	windows	4 <sup>✎</sup>	<sup>✕</sup>

共 1 项

每页显示行 20 <sup>▼</sup> ⏪ ⏩ 1/1 ⏪ ⏩

# 网络流日志

最近更新时间：2024-04-19 16:50:01

网络流日志（Flow logs）为您提供全时、全流、非侵入的流量采集服务，可将采集的网络流量进行实时的存储、分析，适用于故障排查、合规审计、架构优化、安全检测等场景，让您的云上网络更加稳定、安全和智能。

您可以创建指定采集范围（例如弹性网卡、NAT 网关、专线网关、云联网跨地域流量）的网络流日志，来采集该范围内传入/传出的流量。创建流日志后，您可以在 [日志服务（CLS）](#) 中查看和检索数据，也可以在高级分析仪表盘中直观查看日志数据。

## ① 说明

目前 NAT 网关、专线网关、云联网跨地域流量流日志处于内测中，如有需要，请提交 [工单申请](#)。

## 常用操作

- [创建流日志](#)
- [主题配置](#)
- [高级分析](#)
- [创建日志集和日志主题](#)
- [删除流日志](#)
- [查看流日志记录](#)

## 流量镜像

### 流量镜像概述

最近更新时间：2023-10-13 10:32:43

流量镜像提供流量采集服务，可将指定采集范围的流量按不同过滤条件过滤，并复制转发至私有网络 VPC 下的 CVM 上，适用于安全审计、风险监测、故障排障、业务分析等场景。

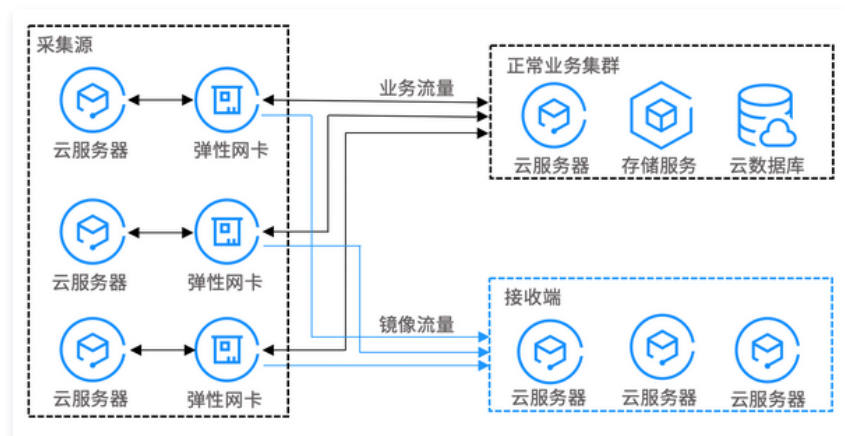
#### 说明

- 使用流量镜像功能，会消耗主机带宽资源。例如某网络接口入站流量和出站流量分别为1Gbps。若该接口使用流量镜像功能，则其应用系统需要处理1Gbps入站流量和3Gbps出站流量（包含1Gbps出站流量、1Gbps镜像入站流量和1Gbps镜像出站流量）。
- 使用流量镜像功能时，请注意相关 CVM 中的流量转发配置（如 ip\_forward 等），避免出现流量环路影响业务稳定。

### 工作流程

流量镜像关键组成为采集源和接收端，具体工作流程如下图所示。

- 采集源：VPC 中指定弹性网卡，可按所属网络、采集范围、采集类型和流量过滤等规则条件进行过滤。
- 接收端：采集流量将被复制转发至接收 IP 中。



### 使用场景

#### 安全审计

在系统运行过程中，由于系统软件处理异常、网络设备硬件故障、计算机病毒或用户不正常使用等原因，造成网络流量异常或产生错误报文。通过流量镜像可以分析网络报文，定位故障产生的原因。

#### 入侵检测

为保证网络系统资源机密性、完整性和可用性，可以使用流量镜像功能将流量复制转发到云服务器集群上，进行实时分析。

#### 业务分析

使用流量镜像功能对业务流量进行镜像，可以清晰可视企业内部业务流量模型。

## 使用限制

最近更新时间：2024-03-20 17:08:41

使用流量镜像前，请根据如下限制进行评估，确保不影响您的业务。

- 目前流量镜像处于内测中，如有需要，请提交 [工单申请](#)，为避免多次申请，建议保存好申请时获取的链接，方便您登录流量镜像控制台。
- 使用流量镜像功能会同比消耗主机 CPU、内存、带宽等资源。  
镜像流量会计入实例带宽，对系统资源的影响取决于您的流量大小和流量类型。例如，某网络接口入站流量和出站流量分别为1Gbps。若该接口使用流量镜像功能，则其应用系统需要处理1Gbps入站流量和3Gbps出站流量（包含1Gbps 出站流量、1Gbps镜像入站流量和1Gbps镜像出站流量）。
- 流日志不能捕获流量镜像数据。
- 安全组限制：
  - 采集源：镜像流量不受安全组策略限制。
  - 接收端：受安全组策略限制。
- 如下数据不能使用流量镜像：
  - 地址解析协议。
  - DHCP。
  - 实例元数据服务。
  - NTP。
  - Windows 激活。
- 流量镜像的采集源端、接收端支持的机型如下：  
标准型 S1、标准型 S2、标准型 S3、内存型 M1、内存型 M2、内存型 M3、高 IO 型 I1、高 IO 型 I2、计算型 C2、计算型 C3、计算增强型 CN3、大数据型 D1。
- 云服务器网卡的限制如下：
  - 在设置流量镜像时，目标服务器的网卡带宽上限至少要大于采集范围内所有服务器网卡带宽总和的 1/9。  
例如：流量镜像采集范围内有6台 S3.6XLARGE48，网卡带宽总和为  $3\text{Gbps} * 6 = 18\text{Gbps}$ 。那么，接收端的入带宽至少为  $2\text{Gbps} (18/9=2)$ 。即至少为2台 S3.MEDIUM8 或1台 S3.4XLARGE32。
  - 为避免镜像流量超过接收端网卡能力，请根据业务流量规模，适当提升接收端的数量和云服务器实例规格，关于云服务器实例规格的详细信息，请参见 [云服务器实例规格](#)。

# 创建流量镜像

最近更新时间：2024-03-20 17:08:41

流量镜像提供流量采集服务，可将指定弹性网卡上的流量按五元组等条件过滤，并复制转发至同 VPC 下的 CVM 上，适用于安全审计、风险监测、故障排障、业务分析等场景。本文将介绍如何创建流量镜像。

**说明：**

目前流量镜像处于内测中，如有需要，请提交 [工单申请](#)，为避免多次申请，建议保存好申请时获取的链接，方便您登录流量镜像控制台。

## 前提条件

请确保被采集流量的 IP 与流量接收 IP 在同一个 VPC 内，且流量采集 IP 有针对流量接收 IP 的路由表。

## 操作步骤

### 步骤一：设置采集流量

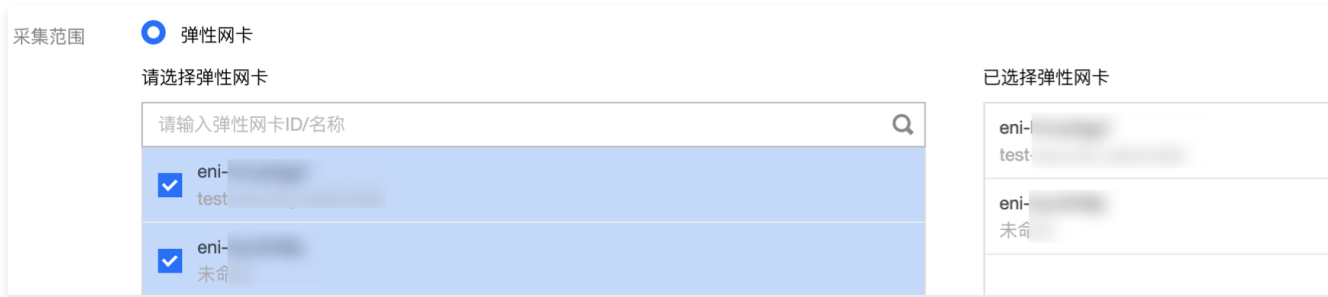
1. 登录 [私有网络控制台](#)。
2. 单击左侧导航栏中的 [诊断工具](#) > [流量镜像](#)，选择待创建流量镜像的地域。
3. 在流量镜像页面单击 [+新建](#)。

**说明：**

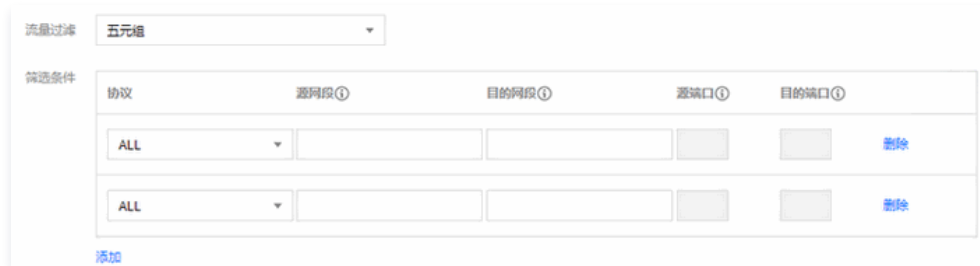
每个 VPC 最多创建5个流量镜像。

4. 在设置采集流量页面进行如下配置：

- 请填写流量镜像的名称，不超过60字符。
- 选择“所属网络”。
- 流量“采集范围”为“弹性网卡”，即采集 VPC 内除目标接收弹性网卡的流量。选择弹性网卡后，需勾选具体弹性网卡。



- 选择“采集类型”：根据业务类型选择采集流量方向，支持“全部流量”、“出流量”和“入流量”。
- 选择“流量过滤”方式：根据业务类型选择流量过滤方式，过滤掉不需要的流量可以减轻镜像的规模和压力。
  - 不过滤：采集配置的全部流量。
  - 五元组：采集满足五元组条件的流量。选择“五元组”后，需设置“协议”、“源网段”、“目的网段”、“源端口”和“目的端口”。若需增加筛选条件，请单击“添加”，多个筛选条件为“与”关系。



- 下一跳为 NAT 网关：采集下一跳为 NAT 网关的流量。选择“下一跳为 NAT 网关”后，需在“筛选条件”右侧选择具体 NAT 网关。

5. 完成配置后，单击“下一步”。

### 步骤二：设置接收流量



1. 在设置接收流量页面配置如下信息：

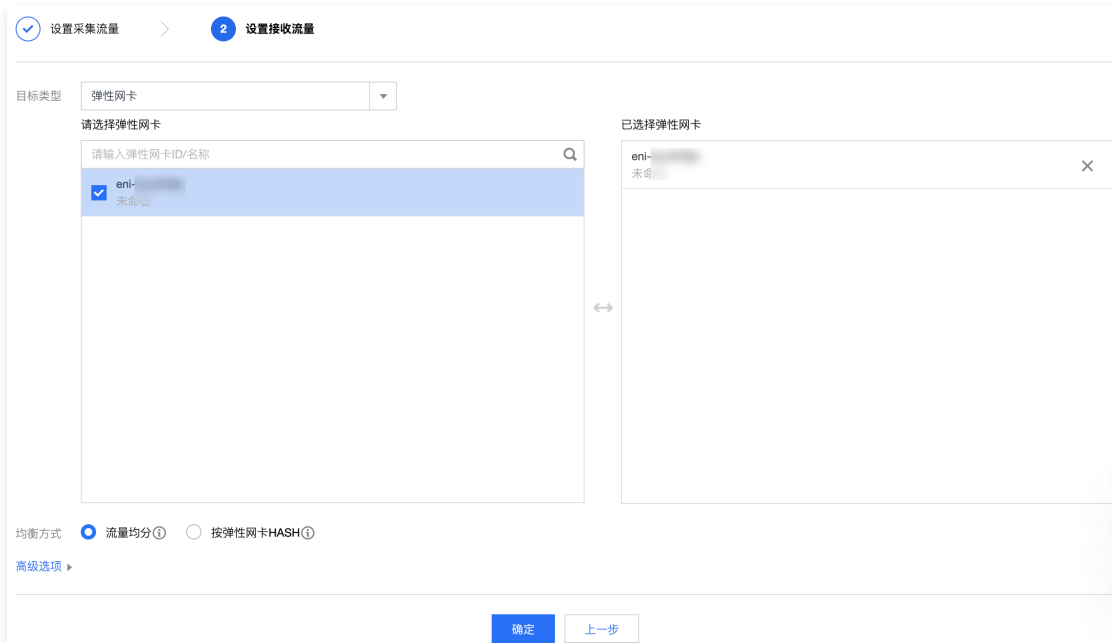
- “目标类型”：选择接收转发流量的目标弹性网卡。

**说明**

- 至少需选择一个目标弹性网卡。
- 在 VPC 内，目标弹性网卡的流量不会被采集。

○ **均衡方式**：选择如下一种方式。

- **流量均分**：所有流量随机均匀分到目标弹性网卡中。
- **按弹性网卡 HASH**：将来自同一个网卡的流量转发到同一个目标弹性网卡中。



2. 完成配置后，单击**确定**。

## 结果验证

**注意：**

本文以采集源端弹性网卡10.0.0.14访问网站 [www.qq.com](http://www.qq.com) 的“出流量”镜像为例。

1. 返回流量镜像页面，创建的流量镜像显示在列表中，且**启用采集**为开启，则表示流量镜像任务创建成功。

名称/ID	采集范围	采集类型	所属网络	创建时间	启用采集	操作
img-...	弹性网卡	全部流量	vpc-...	2022-03-09 11:17:24	<input checked="" type="checkbox"/>	<a href="#">编辑标签</a> <a href="#">删除</a>

2. 执 如下操作，验证采集端的流量是否正常镜像到接收端。

2.1 构造弹性网卡流量，例如您可以登录采集源端 CVM，执行 ping 公网 IP来构造流量。

**source 源数据：**

```
[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 登录接收端云服务器，执行如下命令抓取数据并保存为“.cap”或“.pcap”文件。本例以“.pcap”为例。

```
tcpdump -i eth0 -w capture-2020-10-27.pcap # 文件名可定义，请根据实际情况填写
```

Destination 数据包:

```
[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 使用终端模拟工具（例如 SecureCRT 等）登录接收端服务器，将步骤ii中保存的文件导出到本地。

```
sz -bye capture-2020-10-27.pcap
```

2.4 使用报解析工具（例如 Wireshark 工具）打开下载到本地的文件“capture-2020-10-27.pcap”获取数据详情，例如，本例中已从镜像接收端云服务器获取到采集源端的出流量12个数据包。

包校验:

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 respon
375	27.524318	10.0.0.14	58.250.137.36	ICMP	98	Echo (ping) request id=0x251b, seq=2/512, ttl=64 (no respon
387	28.525991	10.0.0.14	58.250.137.36	ICMP	98	Echo (ping) request id=0x251b, seq=3/768, ttl=64 (no respon
409	29.527690	10.0.0.14	58.250.137.36	ICMP	98	Echo (ping) request id=0x251b, seq=4/1024, ttl=64 (no respo
426	30.529380	10.0.0.14	58.250.137.36	ICMP	98	Echo (ping) request id=0x251b, seq=5/1280, ttl=64 (no respo
443	31.531020	10.0.0.14	58.250.137.36	ICMP	98	Echo (ping) request id=0x251b, seq=6/1536, ttl=64 (no respo
465	32.532644	10.0.0.14	58.250.137.36	ICMP	98	Echo (ping) request id=0x251b, seq=7/1792, ttl=64 (no respo
482	33.534324	10.0.0.14	58.250.137.36	ICMP	98	Echo (ping) request id=0x251b, seq=8/2048, ttl=64 (no respo
487	34.535641	10.0.0.14	58.250.137.36	ICMP	98	Echo (ping) request id=0x251b, seq=9/2304, ttl=64 (no respo
503	35.536630	10.0.0.14	58.250.137.36	ICMP	98	Echo (ping) request id=0x251b, seq=10/2560, ttl=64 (no resp
518	36.537354	10.0.0.14	58.250.137.36	ICMP	98	Echo (ping) request id=0x251b, seq=11/2816, ttl=64 (no resp
541	37.538718	10.0.0.14	58.250.137.36	ICMP	98	Echo (ping) request id=0x251b, seq=12/3072, ttl=64 (no resp

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 40 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  .${%...(.
0030  00 00 25 0d 0e 00 00 00 00 00 10 11 12 13 14 15  .%...
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  .!#$%
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,-./012345
0060  36 37 67
    
```

3. 如获取到数据包异常或 无法正常获取到数据包, 请 [联系我们](#) 或 [在线咨询](#)。

后续步骤

- [启停流量镜像](#)
- [修改流量镜像](#)
- [添加标签](#)
- [删除流量镜像](#)

## 管理流量镜像

最近更新时间：2023-10-27 14:27:35

创建流量镜像后，您可以在控制台进行启停流量镜像、修改流量镜像、添加标签和删除流量镜像等操作。

### 启停流量镜像

创建流量镜像后，默认开启流量镜像任务。您可以参考以下步骤关闭以及再次开启流量镜像。

1. 登录 [私有网络控制台](#)。
2. 单击左侧导航栏中的 **诊断工具** > **流量镜像**，选择待创建流量镜像的地域。
3. 在流量镜像列表中目标流量镜像右侧**启用采集**列下，关闭或开启流量镜像。

名称/ID	采集范围	采集类型	所属网络	创建时间	启用采集	操作
imgf-ccc	弹性网卡	全部流量	vpc-	2021-07-08 10:49:13	<input checked="" type="checkbox"/>	<a href="#">编辑标签</a> <a href="#">删除</a>
imgf-xx	弹性网卡	全部流量	vpc-	2021-09-07 17:17:04	<input checked="" type="checkbox"/>	<a href="#">编辑标签</a> <a href="#">删除</a>

### 修改流量镜像

若需修改已创建的镜像流量，操作步骤如下：

1. 登录 [私有网络控制台](#)。
2. 单击左侧导航栏中的 **诊断工具** > **流量镜像**，选择待创建流量镜像的地域。
3. 在流量镜像列表中，单击目标流量镜像 ID。
4. 选择需更新的模块并进行编辑。
  - 编辑“采集流量”
    - a. 在采集流量模块右上角单击**编辑**。
    - b. 在弹出的“编辑采集流量”窗口中，修改“采集弹性网卡”、“采集类型”和“流量过滤”等参数，完成后单击**确定**。
  - 编辑“接收流量”
    - a. 在接收流量模块右上角单击**编辑**。
    - b. 在弹出的“编辑接收 IP”窗口中，修改“目标弹性网卡”和“均衡方式”，完成后单击**确认**。

#### 采集流量 编辑

采集弹性网卡

ID/名称
eni-tes

采集类型 全部流量

流量过滤 不过滤

#### 接收流量 编辑

目标类型 弹性网卡ENI

弹性网卡ENI

ID/名称
eni-未命
eni-未命

均衡方式 按弹性网卡HASH <sup>①</sup>

### 添加标签

标签用于标识和组织腾讯云资源，每一个标签包含一个标签键和一个标签值。为流量镜像添加标签可便于筛选和管理流量镜像资源。

1. 登录 [私有网络控制台](#)。
2. 单击左侧导航栏中的 **诊断工具** > **流量镜像**，选择待创建流量镜像的地域。
3. 在流量镜像列表中，单击目标流量镜像右侧**操作**列下的**编辑标签**。
4. 在弹出对话框中进行以下操作：
  - 4.1 在**标签键**列输入标签键。您也可以在下拉列表中选择已创建的标签键。
  - 4.2 在**标签值**列输入标签值。

#### 说明

标签值可为空，一个标签键可以包含多个标签值。

4.3（可选）若需创建多个标签，请单击添加并编辑标签键和标签值。

4.4 完成添加后，单击确定。

## 查找流量镜像

1. 在流量镜像页面右上角单击 ，单击选择过滤属性。系统支持如下3种过滤属性。



2. 在编辑框中输入属性值，并单击 。

 说明  
多个属性值用“|”隔开。

## 删除流量镜像

1. 登录 [私有网络控制台](#)。
2. 单击左侧导航栏中的 [诊断工具](#) > [流量镜像](#)，选择待创建流量镜像的地域。
3. 在流量镜像列表中，单击目标流量镜像右侧操作列下的删除，并确认操作即可。

## 快照策略

### 概述

最近更新时间：2023-10-27 14:27:35

通过快照功能可对其关联的对象数据按照设定的备份策略进行备份。目前快照支持关联安全组，关联后可对安全组出、入站规则进行备份，该功能为辅助功能，不会影响安全组的相关操作。

### 应用场景

如果您的安全组规则经常需要更新，我们建议您为安全组配置快照策略，及时备份安全组规则数据，当新修改的安全组规则出现异常，需要恢复到原来的规则时，可利用快照回滚功能，将安全组规则恢复至已快照备份的规则状态，从而保证业务的可用性。

### 使用限制

资源	配额
每个用户最多可创建的快照策略数	5
每个定时快照策略中可设置的时间节点	5
单对象（安全组）可关联的快照策略数	1
单快照策略可关联的对象（安全组）数量	50
定时快照策略保留时间上限	365天
变更备份的变更频率	10秒5次

# 创建快照策略

最近更新时间：2023-10-27 14:27:35

当您需要对安全组规则进行备份，以便后续因业务需要，或新规则异常需要回退到原安全组规则时，可为安全组规则配置快照策略，实现对安全组规则的备份。

### 注意

授权 COS 服务：由于快照记录存放在 COS 存储桶中，需要对 COS 进行读写操作，因此在创建快照策略时，如您未授权过 COS 服务，系统会自动弹出授权窗口，请您按照界面提示进行授权，完成授权后重新刷新即可进入快照策略界面，后续无需重复授权。

## 操作步骤

1. 登录 [私有网络控制台](#)，选择左侧导航栏的 **诊断工具 > 快照策略**，进入快照策略界面。
2. 单击 **新建**，进入新建快照策略界面。



3. 在 **新建快照策略** 界面，配置快照策略相关参数。

**新建快照策略** ✕

*快照策略当前不收费，由于备份数据存储在存储桶中，cos存储桶将对此部分数据收费，详情查看[对象存储计费概述](#)*

名称

备份策略  操作备份  定时备份

快照保留时间 保留  天后自动删除

创建新的cos存储桶  是  否

COS桶所属地域

COS桶名称  仅支持小写字母、数字和-的组合，域名字数总和不能超过60字符，存储桶名称一旦设置不能更改

参数	说明
名称	自定义填写快照策略的名称，支持数字、字母与字符的组合。
备份策略	<p>支持操作备份、定时备份两种方式：</p> <ul style="list-style-type: none"> <li>操作备份：指每次对安全组规则进行“操作”时会触发备份。</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <p><b>注意：</b> 目前变更操作的频率限制是10秒5次，过于频繁的操作将不会被全部记录。</p> </div> <ul style="list-style-type: none"> <li>定时备份：固定时间点进行备份。</li> </ul>

备份时间	仅选择 <b>定时备份</b> 时，会展示该参数。日期支持选择周一到周日，时间可精确到秒，最多可添加5个备份时间，至少保留1个备份时间。 <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <b>注意：</b>                      备份操作受数据量影响，当数据量较大时，选择时间点与实际完成备份时间点可能存在部分偏差。                 </div>
快照保留时间	支持自定义备份记录的保留时间，超过保留时间后，记录自动删除。最长保留时间为365天。
创建新的 COS 存储桶	<ul style="list-style-type: none"> <li>是：新建 COS 存储桶。</li> <li>否：现有 COS 存储桶。</li> </ul>
COS 存储桶	<ul style="list-style-type: none"> <li>如选择新建 COS 存储桶，请选择地域，并填写 COS 存储桶名称，名称一旦设置不能更改。仅支持小写字母、数字和“-”的组合，且域名字数总和不能超过60字符。</li> <li>如选择现有 COS 存储桶，请选择地域及具体存储桶名称，选定后不支持更改，请妥善选择。</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <b>注意：</b>                      备份信息保存于 COS 存储桶内，当存储桶删除后将导致快照信息无法查询与恢复。                 </div>
COS 桶名称	存储桶名称由自定义名称 - 开发商 AppID 构成。仅支持小写字母、数字和 - 的组合，域名字数总和不能超过60字符，存储桶名称一旦设置不能更改。

4. 单击**确定**完成快照策略的配置。

## 后续操作

[关联安全组](#)



## 关联、解绑、查询安全组

最近更新时间：2023-10-27 14:27:35

快照策略创建后，可关联安全组，加入到快照列表的安全组，将按照设定的快照策略进行备份，不需要对安全组进行快照备份时，可以解绑安全组。本章节介绍如何为快照策略关联和解绑安全组，以及如何查看已关联的安全组。

### 前提条件

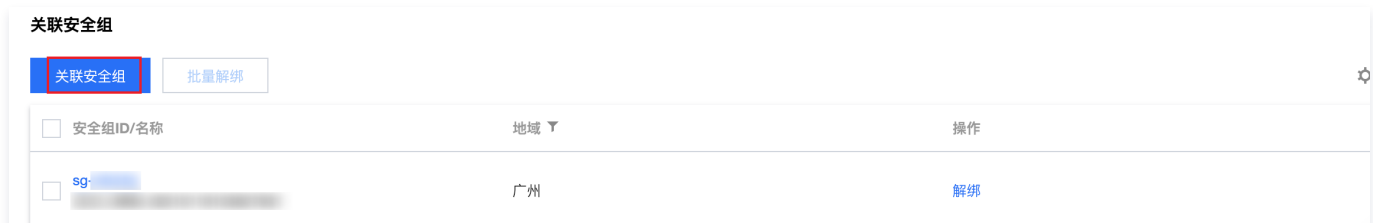
- 已创建快照策略。
- 已准备好待关联的安全组。

### 关联安全组

1. 登录 [私有网络控制台](#)，选择左侧导航栏的**诊断工具 > 快照策略**，进入快照策略界面。
2. 在快照策略界面，单击快照策略 ID，进入详情界面。



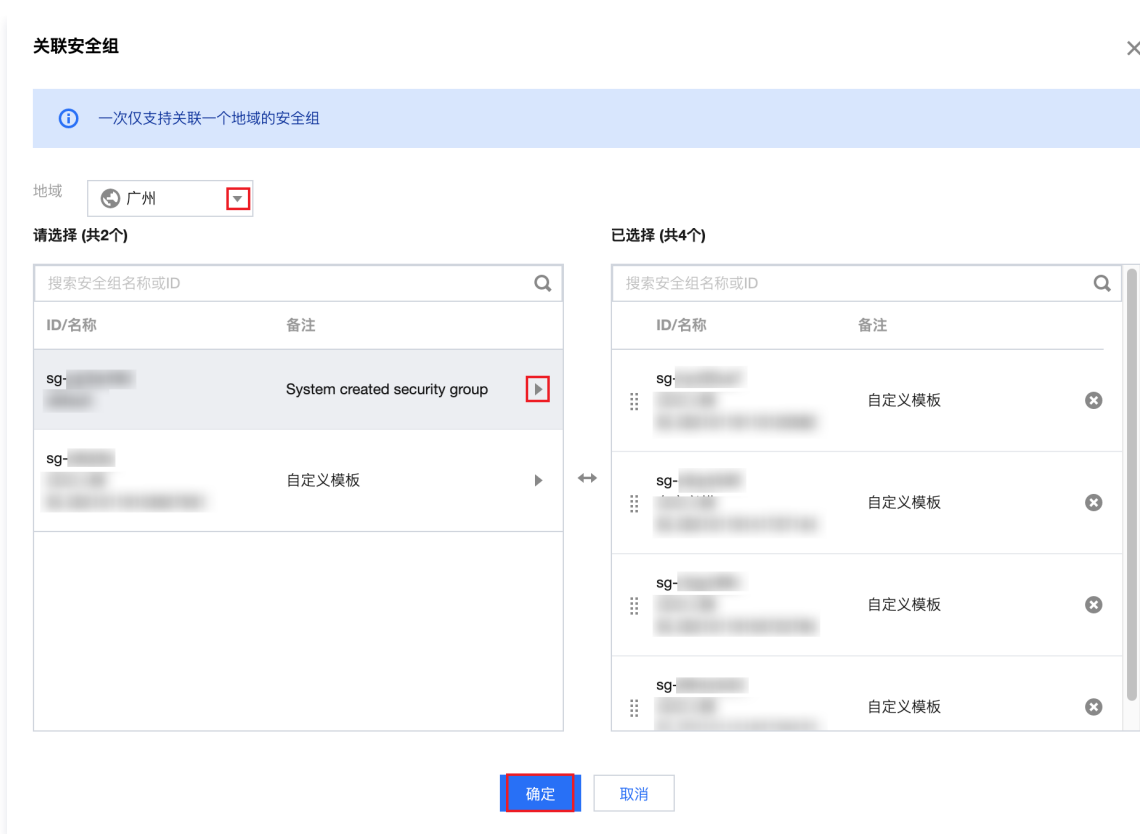
3. 单击**关联安全组**。



4. 在**关联安全组**界面，选择**地域**，并单击**请选择**列表中待关联安全组右侧的三角图标，已选定的安全组展示在右侧**已选择**列表中，完成后单击**确定**。

#### 说明

- 快照策略无地域属性，可关联所有地域的安全组实例，但单次仅支持关联一个地域的安全组，如需关联多个地域的安全组，可多次执行关联安全组操作。
- 一个安全组仅能关联到一个快照策略上。

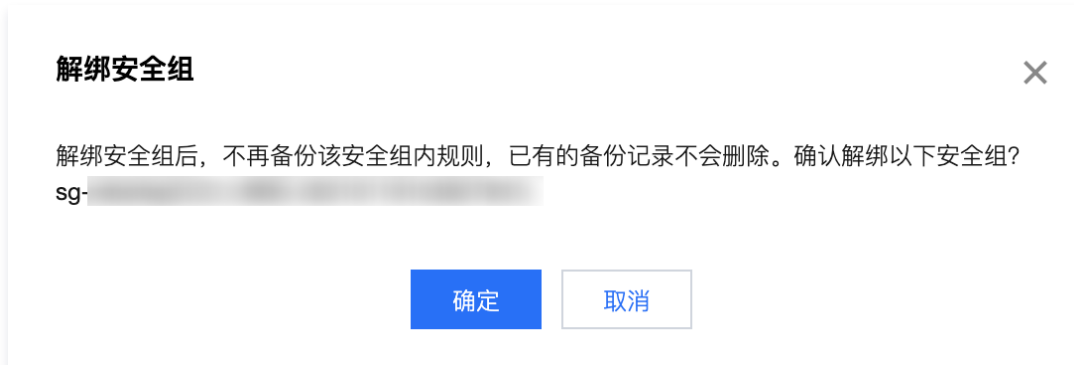


### 解绑安全组

1. 登录 [私有网络控制台](#)，选择左侧导航栏的 **诊断工具 > 快照策略**，进入快照策略界面。
2. 在快照策略界面，单击快照策略 ID，进入详情界面。
3. 单击待解绑的安全组右侧的 **解绑**。



4. 在弹出的 **解绑安全组** 对话框中，确认解绑信息，并单击 **确定** 即可完成安全组解绑，解绑后将不再备份该安全组规则，已有的备份记录不会删除。



5. (可选) 如需同时解绑多个安全组，可勾选安全组，并单击上方的 **批量解绑**，在弹出的确认对话框中单击 **确定** 即可。

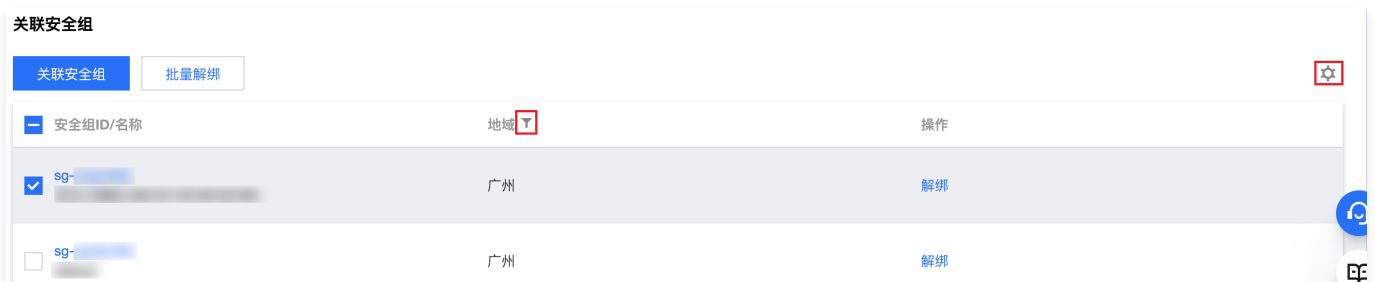
**说明**  
一次只能批量解绑一个地域的多个安全组。



## 查询安全组

如需查询快照策略已关联的安全组，可参考本操作。

1. 登录 [私有网络控制台](#)，选择左侧导航栏的 [诊断工具](#) > [快照策略](#)，进入快照策略界面。
2. 在快照策略界面，单击快照策略 ID，进入详情界面。
3. 在 **关联安全组** 区域，将展示该快照策略关联的所有安全组。
4. 单击地域旁的筛选图标，可按地域筛选安全组，单击右上角的设置图标，可自定义列表字段。



5. 单击安全组 ID，可跳转到安全组详情页。

## 启用和关闭快照策略

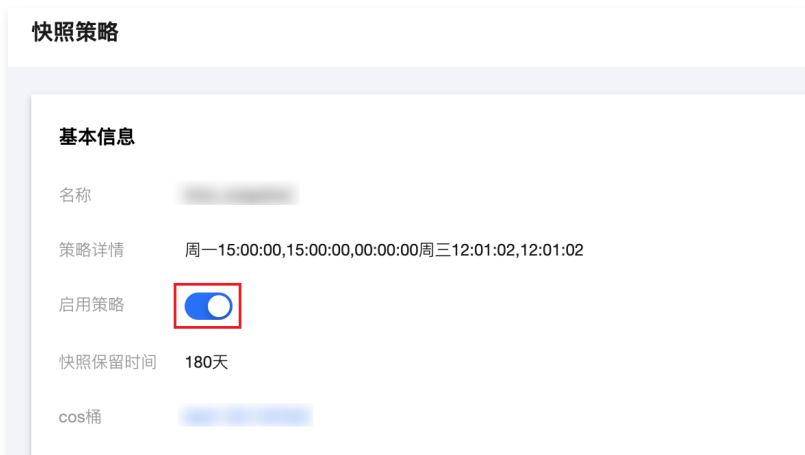
最近更新时间：2023-10-27 14:27:35

快照策略创建成功后，策略是默认开启的，如因业务需要，需暂时停止快照策略中关联的所有安全组的快照备份，且不希望删除原有的备份信息，可参考本章节暂时关闭策略，当需要启用时再重新启用。

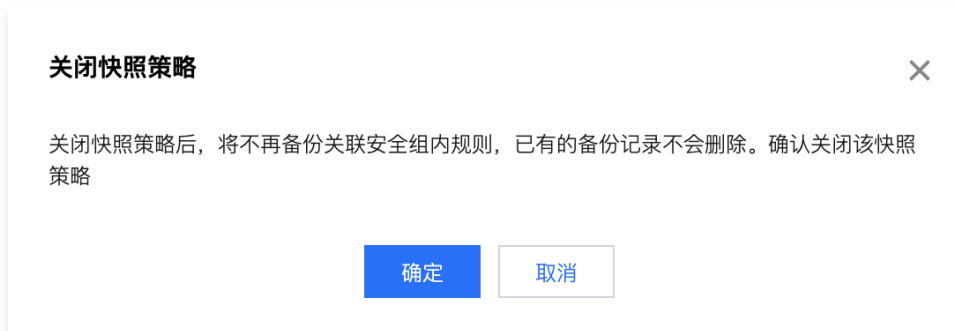
### 关闭策略

关闭策略后不再进行备份，原备份信息不会删除。

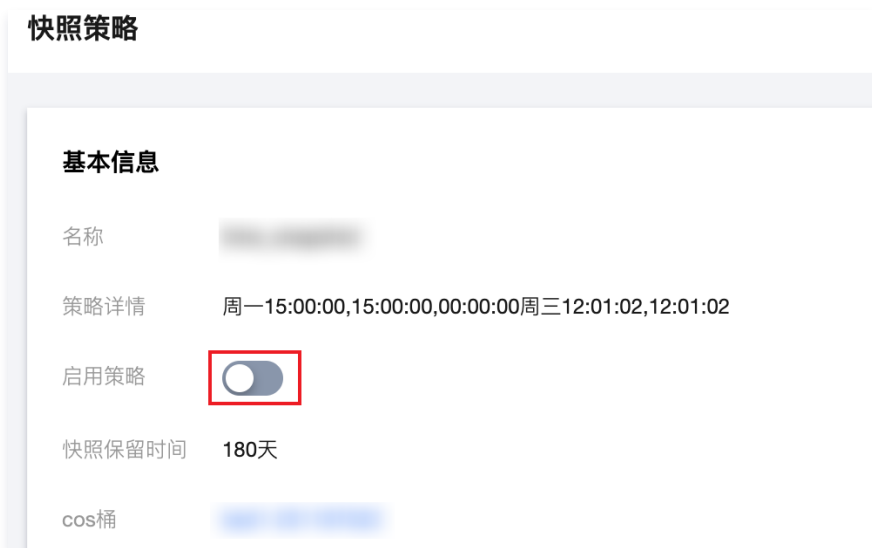
1. 登录 [私有网络控制台](#)，选择左侧导航栏的**诊断工具** > **快照策略**，进入快照策略界面。
2. 在**快照策略**界面，单击快照策略 ID，进入详情界面，图中蓝色图标表示策略启用中。



3. 单击该图标，并在弹出的**关闭快照策略**对话框，确认关闭策略的影响，然后单击**确定**即可关闭快照策略。



关闭后如下图所示：



### 启用策略

策略关闭后，如需重新启用，可参考如下操作，启用后，将继续按照原先设定的策略备份关联的安全组规则。

1. 单击**启用策略**为关闭状态的图标。
2. 在弹出的**启用快照策略**对话框中，单击**确定**即可启用快照策略。

## 修改快照策略

最近更新时间：2023-10-27 14:27:35

用户可对快照策略的名称、保留时间，以及备份时间进行修改，具体请参考如下操作步骤。

## 操作步骤

1. 登录 [私有网络控制台](#)，选择左侧导航栏的**诊断工具 > 快照策略**，进入快照策略界面。
2. 在快照策略界面，单击待修改策略右侧的**修改策略**。

ID/名称	cos存储桶	备份策略	保留时间	创建时间	状态	操作
[模糊]	[模糊]	周一 15:00:00,15:00:00,00:00:00 周三12:01:02,12:01:02	180天	2021-10-09 17:08:19	开启	<a href="#">修改策略</a> <a href="#">删除</a>

3. 在弹出的**修改快照策略**对话框中，根据业务实际情况进行修改。

- 如果是**操作备份**，则支持修改策略名称和快照保留时间。

### 修改快照策略 ✕

名称

快照保留时间 保留  天后自动删除

- 如果是**定时备份**，则支持修改策略名称、备份时间，以及快照保留时间。

### 修改快照策略 ✕

名称  ✔

备份时间

日期	时间
周一 ▾	15:00:00 <span>🕒</span>
周一 ▾	00:00:00 <span>🕒</span> <span style="color: red;">✕</span>

+ 添加

快照保留时间 保留  天后自动删除

4. 单击**确定**完成修改操作。

## 查询快照策略



最近更新时间：2023-10-27 14:27:35

快照策略界面展示所有已创建的快照策略详情信息，包括策略名称、COS 存储桶、备份策略、保留时间、创建时间、策略状态、及相关可执行的操作等信息。

### 操作步骤

1. 登录 [私有网络控制台](#)，选择左侧导航栏的**诊断工具 > 快照策略**，进入快照策略界面。
2. 进入快照策略界面，所有已创建的快照策略展示在列表中。

ID/名称	cos存储桶	备份策略	保留时间	创建时间	状态	操作
		周一 15:00:00,15:00:00,00:00:00 周三12:01:02,12:01:02	180天	2021-10-09 17:08:19	开启	修改策略 删除
		每次变更自动创建快照	180天	2021-10-08 16:09:46	开启	修改策略 删除

- 单击策略 ID，可进入具体策略详情查看策略基本信息，及已关联的安全组。
- 单击 COS 存储桶名称，可查看存储桶详情。
- 单击右上角  的图标，可自定义列表字段。
- 单击右上角的  图标，可刷新界面显示信息。

## 删除快照策略

最近更新时间：2023-10-27 14:27:35

如不再需要对安全组进行快照备份，且需要删除快照策略关联的所有安全组规则的备份记录，可参考如下步骤删除快照策略。

### 操作步骤

1. 登录 [私有网络控制台](#)，选择左侧导航栏的**诊断工具** > **快照策略**，进入快照策略界面。
2. 在快照策略界面，单击需要删除的快照策略右侧的**删除**。
3. 在删除确认对话框中，确认删除后的影响，确认无误后，再单击**确定**。

#### 注意

删除后将不再对快照策略中关联的所有安全组规则进行备份，且会删除已有的备份记录，请谨慎操作。



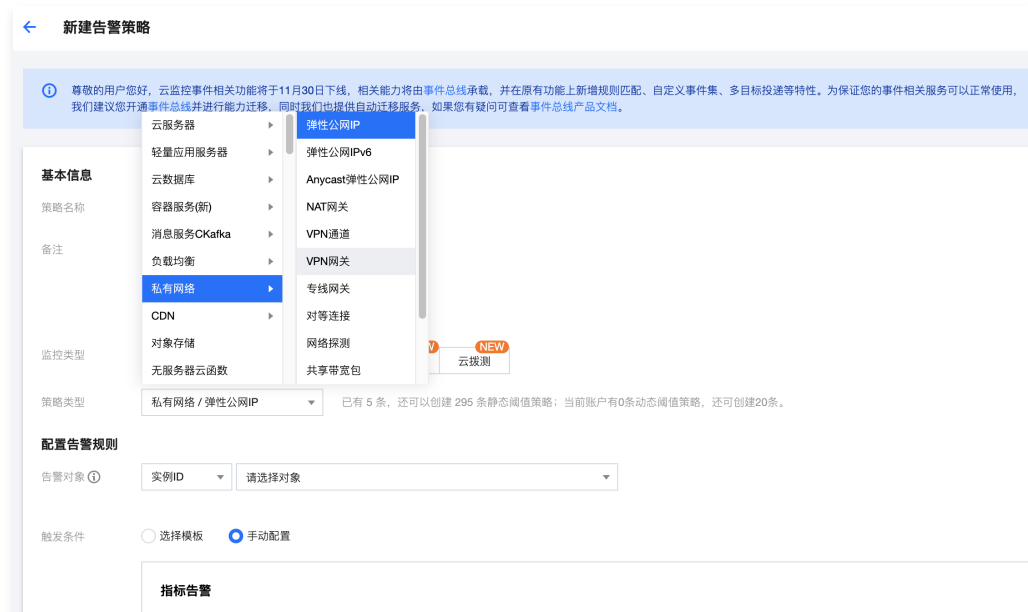
# 告警与监控

最近更新时间：2023-10-24 16:59:31

您可以为私有网络内云资源，如 NAT 网关、VPN 网关、专线网关、EIP 等配置告警策略，来监控并上报云资源的指标状态，以便及时发现云资源的运行异常，尽快定位并解决问题，提升运维效率。

## 配置告警

1. 登录 [腾讯云可观测平台](#)。
2. 单击**告警管理**，在告警管理页的顶部菜单，切换为策略管理菜单。
3. 单击**新建**，填写告警策略名称、策略类型选择需要配置告警的私有网络云资源，例如**私有网络 > 弹性公网 IP**，再根据实际情况配置告警规则和告警通知。



4. 单击**完成**，即可在告警策略列表中查看已设置的告警策略。

### 说明

告警策略创建后，需要解绑所有资源才能删除。

5. 告警条件出发后，您将通过已选择的告警渠道接收到告警通知（短信 / 邮件 / 站内信等）。

各云资源详细配置请参见：

- [配置专线接入告警](#)
- [配置云联网告警](#)
- [配置 NAT 网关告警](#)
- [配置对等连接告警](#)
- [配置 VPN 连接告警](#)

## 查看监控

您可以在私有网络云资源控制台查看相应云资源的监控数据，帮助您排查网络故障，请参见：

- [查看专线监控信息](#)
- [查看云联网监控信息](#)
- [查看 NAT 网关监控信息](#)
- [查看对等连接监控信息](#)
- [查看 VPN 连接监控信息](#)
- [查看弹性公网 IP 监控信息](#)

# API 2.0 切换 API 3.0 指引

最近更新时间：2023-06-20 11:20:35

私有网络 API 已全面升级至3.0版本，基于2.0版本接口访问时延较高和使用复杂的考虑，原私有网络 API 2.0 接口服务将不再提供技术支持，并于2023年01月01日起下线。如果您的业务还在使用私有网络 API 2.0 相关接口，建议尽快将服务升级至 API 3.0 接口，以免对您的业务造成影响。

请您参照如下对比，找到您需要升级的新接口，完成升级：

- 2.0文档：[API 概览](#)
- 3.0文档：[API 概览](#)

## API 2.0 切换3.0接口列表

### 私有网络

接口功能	API 2.0	API 3.0	备注
创建私有网络	<a href="#">CreateVpc</a>	<a href="#">CreateVpc</a>	-
删除私有网络	<a href="#">DeleteVpc</a>	<a href="#">DeleteVpc</a>	-
修改私有网络名称	<a href="#">ModifyVpcAttribute</a>	<a href="#">ModifyVpcAttribute</a>	-
查询私有网络列表	<a href="#">DescribeVpcEx</a>	<a href="#">DescribeVpcs</a>	-
绑定私有网络内主机与 VIP	<a href="#">AssociateVip</a>	/	本接口实现的功能已经用弹性网卡功能代替，不推荐使用该接口
创建私有网络和基础网络设备互通	<a href="#">AttachClassicLinkVpc</a>	<a href="#">AttachClassicLinkVpc</a>	-
删除私有网络和基础网络设备互通	<a href="#">DetachClassicLinkVpc</a>	<a href="#">DetachClassicLinkVpc</a>	-
查询私有网络和基础网络设备互通	<a href="#">DescribeVpcClassicLink</a>	<a href="#">DescribeClassicLinkInstances</a>	-

### 子网

接口功能	API 2.0	API 3.0
创建子网	<a href="#">CreateSubnet</a>	<a href="#">CreateSubnet</a>
删除子网	<a href="#">DeleteSubnet</a>	<a href="#">DeleteSubnet</a>
修改子网名称	<a href="#">ModifySubnetAttribute</a>	<a href="#">ModifySubnetAttribute</a>
查询子网列表	<a href="#">DescribeSubnetEx</a>	<a href="#">DescribeSubnets</a>
查询子网详情	<a href="#">DescribeSubnet</a>	<a href="#">DescribeSubnets</a>

### 路由表

接口功能	API 2.0	API 3.0
创建路由表	<a href="#">CreateRouteTable</a>	<a href="#">CreateRouteTable</a>
删除路由表	<a href="#">DeleteRouteTable</a>	<a href="#">DeleteRouteTable</a>
修改路由表	<a href="#">ModifyRouteTableAttribute</a>	<a href="#">ModifyRouteTableAttribute</a>
查询路由表	<a href="#">DescribeRouteTable</a>	<a href="#">DescribeRouteTables</a>
修改子网关联的路由表	<a href="#">AssociateRouteTable</a>	<a href="#">ReplaceRouteTableAssociation</a>
添加路由策略	<a href="#">CreateRoute</a>	<a href="#">CreateRoutes</a>
删除路由策略	<a href="#">DeleteRoute</a>	<a href="#">DeleteRoutes</a>

## 网络 ACL

接口功能	API 2.0	API 3.0
创建 VPC 网络 ACL	<a href="#">CreateNetworkAcl</a>	<a href="#">CreateNetworkAcl</a>
删除网络 ACL	<a href="#">DeleteNetworkAcl</a>	<a href="#">DeleteNetworkAcl</a>
修改网络 ACL 名称	<a href="#">ModifyNetworkAcl</a>	<a href="#">ModifyNetworkAclAttribute</a>
查询网络 ACL 列表	<a href="#">DescribeNetworkAcl</a>	<a href="#">DescribeNetworkAcls</a>
设置网络 ACL 规则	<a href="#">ModifyNetworkAclEntry</a>	<a href="#">ModifyNetworkAclEntries</a>
网络 ACL 绑定子网	<a href="#">CreateSubnetAclRule</a>	<a href="#">AssociateNetworkAclSubnets</a>
网络 ACL 解绑子网	<a href="#">DeleteSubnetAclRule</a>	<a href="#">DisassociateNetworkAclSubnets</a>

## 弹性网卡

接口功能	API 2.0	API 3.0
创建弹性网卡	<a href="#">CreateNetworkInterface</a>	<a href="#">CreateNetworkInterface</a>
删除弹性网卡	<a href="#">DeleteNetworkInterface</a>	<a href="#">DeleteNetworkInterface</a>
查询弹性网卡信息	<a href="#">DescribeNetworkInterfaces</a>	<a href="#">DescribeNetworkInterfaces</a>
弹性网卡申请内网 IP	<a href="#">AssignPrivateIpAddresses</a>	<a href="#">AssignPrivateIpAddresses</a>
弹性网卡退还内网 IP	<a href="#">UnassignPrivateIpAddresses</a>	<a href="#">UnassignPrivateIpAddresses</a>
弹性网卡绑定云服务器	<a href="#">AttachNetworkInterface</a>	<a href="#">AttachNetworkInterface</a>
弹性网卡解绑云服务器	<a href="#">DetachNetworkInterface</a>	<a href="#">DetachNetworkInterface</a>
弹性网卡迁移	<a href="#">MigrateNetworkInterface</a>	<a href="#">MigrateNetworkInterface</a>
内网 IP 迁移	<a href="#">MigratePrivateIpAddress</a>	<a href="#">MigratePrivateIpAddress</a>

## 安全组

接口功能	API 2.0	API 3.0	备注
查询实例关联安全组	<a href="#">DescribeInstancesOfSecurityGroup</a>	<a href="#">DescribeInstances</a>	Filter参数带security-group-id
查询安全组规则	<a href="#">DescribeSecurityGroupPolicies/DescribeSecurityGroupPolicy</a>	<a href="#">DescribeSecurityGroupPolicies</a>	-
删除安全组	<a href="#">DeleteSecurityGroup</a>	<a href="#">DeleteSecurityGroup</a>	-
查看安全组	<a href="#">DescribeSecurityGroupEx/DescribeSecurityGroups</a>	<a href="#">DescribeSecurityGroups</a>	-
替换单条安全组规则	<a href="#">ModifySingleSecurityGroupPolicy</a>	<a href="#">ReplaceSecurityGroupPolicy</a>	-
修改安全组出站和入站规则	<a href="#">ModifySecurityGroupPolicy</a>	<a href="#">ModifySecurityGroupPolicies</a>	-
查询网卡关联安全组	<a href="#">DescribeNetworkInterfacesOfSecurityGroup</a>	<a href="#">DescribeNetworkInterfaces</a>	Filter参数带groups.security-group-id
添加安全组规则	<a href="#">CreateSecurityGroupPolicy</a>	<a href="#">CreateSecurityGroupPolicies</a>	-

## 其他

接口功能	API 2.0	API 3.0
查询VPC异步任务执行结果	<a href="#">DescribeVpcTaskResult</a>	<a href="#">DescribeVpcTaskResult</a>
查询账户属性	<a href="#">DescribeAccountVpcAttributes</a>	<a href="#">DescribeAccountAttributes</a>