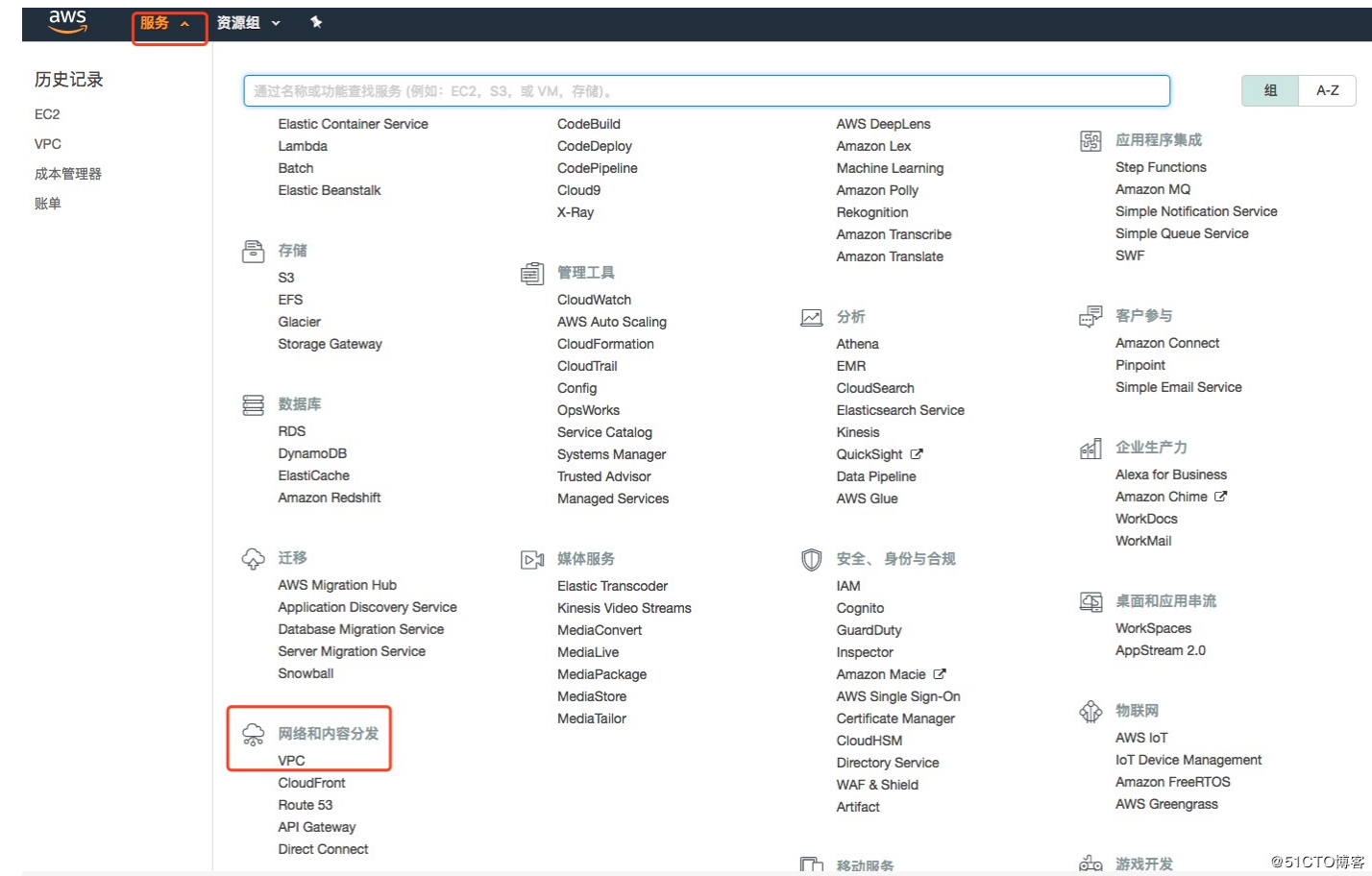


1、创建VPC

服务中找到网路与内容分发，点击VPC，再点击“1个VPC”，进入VPC管理控制台，进来后会看到一个默认的VPC



**VPC 控制面板**  
用 VPC 筛选  
Q 选择 VPC

Virtual Private Cloud

您的 VPC

子网  
路由表  
Internet 网关  
仅出口 Internet 网关  
DHCP 选项集  
弹性 IP  
终端节点  
终端节点服务  
NAT 网关  
对等连接

安全性  
网络 ACL  
安全组

VPN 连接  
客户网关  
虚拟专用网关  
VPN 连接

**资源**

启动 VPC 向导 启动 EC2 实例

注意：您的实例将在美国东部 (俄亥俄) 区域中启动。

您正在使用以下在 美国东部 (俄亥俄) 区域中的 Amazon VPC 资源：

- 1 个 VPC
- 0 个仅出口 Internet 网关
- 1 个路由表
- 0 个弹性 IP
- 0 个终端节点
- 1 个安全组
- 0 个 VPN 连接
- 0 个客户网关
- 1 个 Internet 网关
- 3 个子网
- 1 个网络 ACL
- 0 个 VPC 对等连接
- 0 个 Nat 网关
- 0 个正在运行的实例
- 0 个虚拟专用网关

**VPN 连接**

通过 Amazon VPC，您可以在 AWS 云内使用您自己的隔离资源，然后使用行业标准加密 IPsec VPN 连接将这些资源直接连接到您自己的数据中心。

创建 VPN 连接

**服务运行状况**

当前状态	详细信息
✓ Amazon VPC - US East (Ohio)	Service is operating normally
✓ Amazon EC2 - US East (Ohio)	Service is operating normally

[查看完整的服务运行状况详细信息](#)

**其他信息**

VPC 文档  
所有 VPC 资源  
论坛  
报告问题

@51CTO博客

**VPC 控制面板**  
用 VPC 筛选  
Q 选择 VPC

Virtual Private Cloud

您的 VPC

子网  
路由表  
Internet 网关  
仅出口 Internet 网关  
DHCP 选项集  
弹性 IP  
终端节点  
终端节点服务  
NAT 网关  
对等连接

安全性  
网络 ACL  
安全组

VPN 连接  
客户网关  
虚拟专用网关  
VPN 连接

创建 VPC 操作

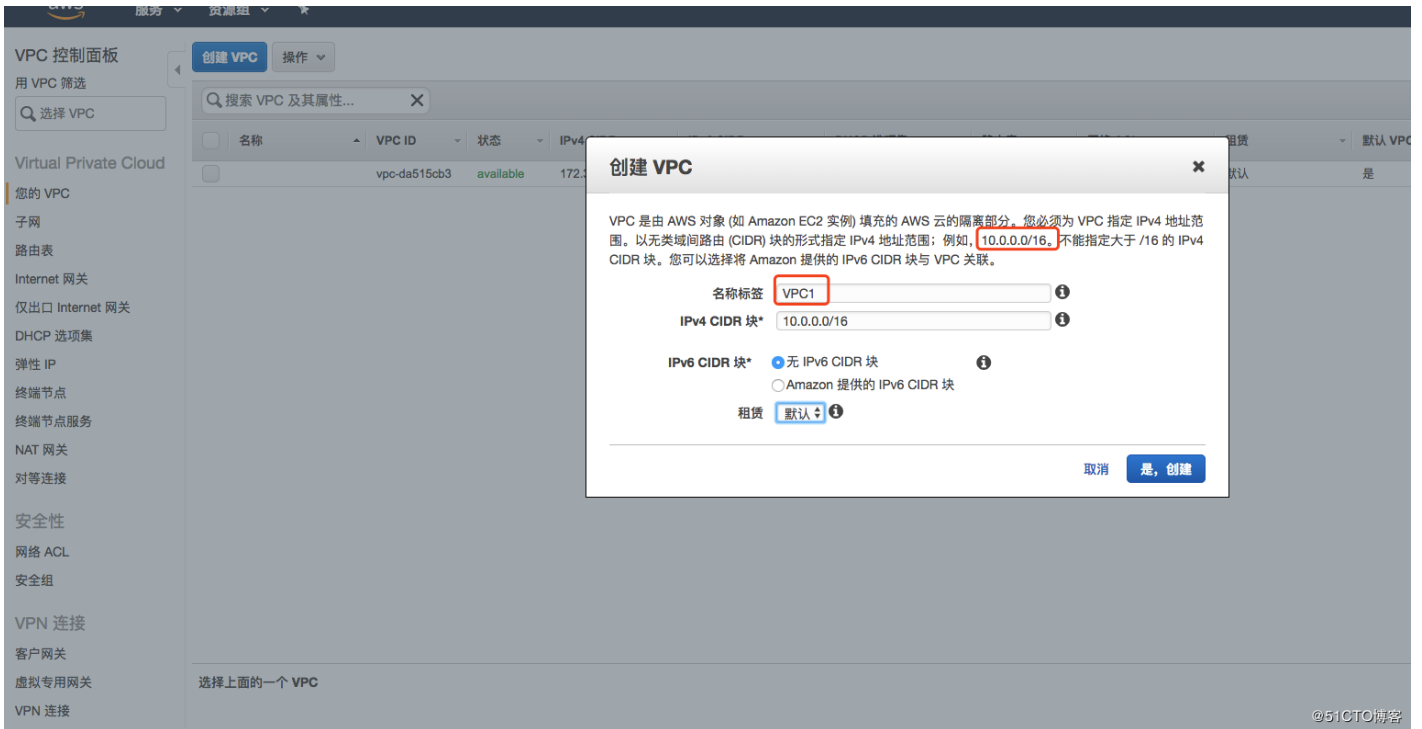
搜索 VPC 及其属性...

名称	VPC ID	状态	IPv4 CIDR	IPv6 CIDR	DHCP 选项集	路由表	网络 ACL	租赁	默认 VPC
	vpc-da515cb3	available	172.31.0.0/16		dopt-4a5d4c23	rtb-4faa4727	acl-e8a5bb81	默认	是

选择上面的一个 VPC

@51CTO博客

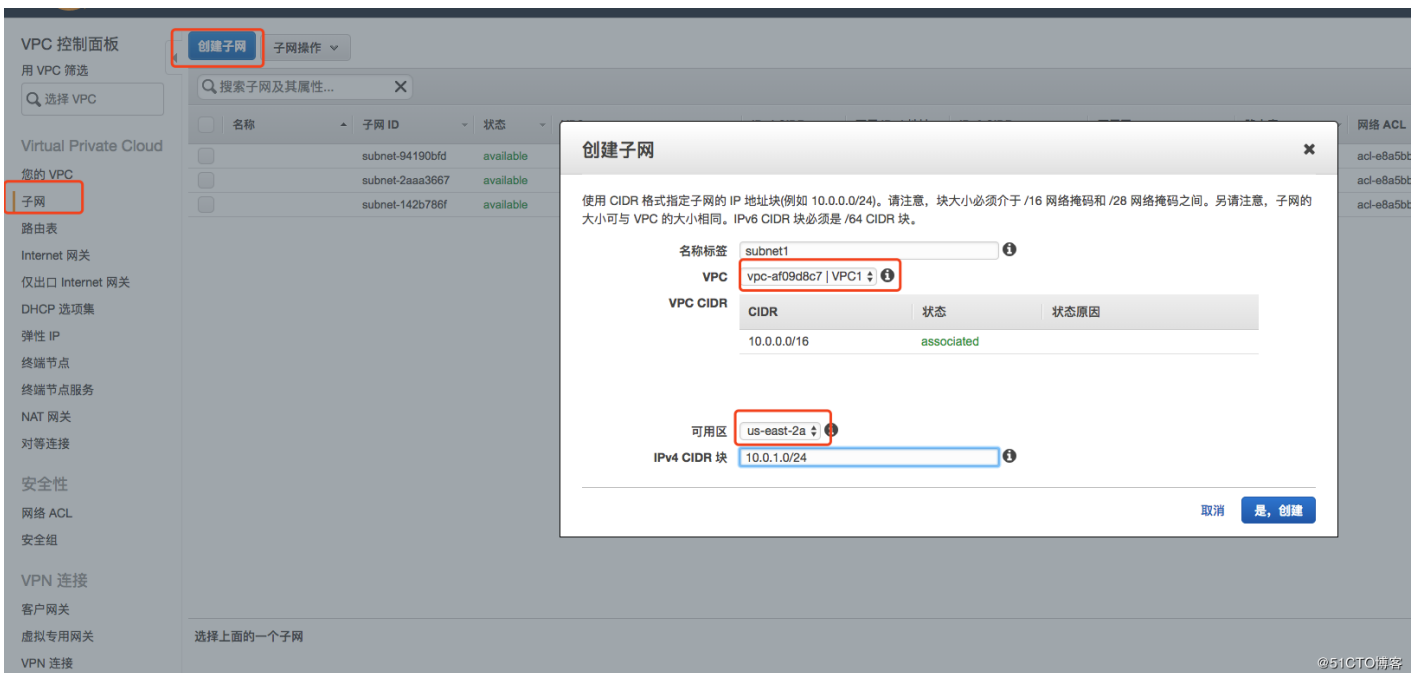
点击创建VPC，注意VPC的网段通常用16位掩码，且不能大于/16，我这里是设置10.0.0.0/16，也可以是其他的，比如：192.168.0.0/16，或者172.16.0.0/16，不同VPC使用不同的地址段



## 2、创建子网

控制台左边点击子网, 点击**创建子网**, 注意创建子网时要选择前面创建的VPC, 而不是默认的VPC, 还要指定一个可用区, 子网的IP地址段一般是24位掩码。

不同的可用区通常使用不同的子网



同样的操作, 再创建一个子网, 关联到us-east-2b

创建子网子网操作

搜索子网及其属性...

<< 1 到 5, 共 5 个子网 >>

<input type="checkbox"/>	名称	子网 ID	状态	VPC	IPv4 CIDR	可用 IPv4 地址	IPv6 CIDR	可用区	路由表	网络 ACL	默认子网	自动
<input checked="" type="checkbox"/>	subnet2	subnet-536b7828	available	vpc-af09d8c7   VPC1	10.0.2.0/24	251		us-east-2b	rtb-c37afcab	acl-3c15bf54	否	否
<input type="checkbox"/>	subnet1	subnet-3669b75e	available	vpc-af09d8c7   VPC1	10.0.1.0/24	251		us-east-2a	rtb-c37afcab	acl-3c15bf54	否	否

@51CTO博客

3、创建IGW网关，并附加到VPC1上

aws 服务 资源组

VPC 控制面板

用 VPC 筛选

选择 VPC

Virtual Private Cloud

您的 VPC

子网

路由表

Internet 网关

仅出口 Internet 网关

DHCP 选项集

弹性 IP

终端节点

终端节点服务

NAT 网关

对等连接

创建 Internet 网关 删除 附加到 VPC 与 VPC 分离

搜索 Internet 网关及其属性...

<input type="checkbox"/>	名称	ID	状态	VPC
<input type="checkbox"/>		igw-fd307794	attached	vpc-da515cb3

创建 Internet 网关

Internet 网关是将 VPC 连接到 Internet 的虚拟路由器。

名称标签 IGW\_for\_VPC1

取消 是, 创建

选择上面的一个 Internet 网关

@51CTO博客

创建 Internet 网关 删除 附加到 VPC 与 VPC 分离

搜索 Internet 网关及其属性...

<input type="checkbox"/>	名称	ID	状态	VPC
<input type="checkbox"/>		igw-fd307794	attached	vpc-da515cb3
<input checked="" type="checkbox"/>	IGW_for_VPC1	igw-5219293b	detached	

@51CTO博客

4、创建路由表

VPC 控制面板

用 VPC 筛选

选择 VPC

Virtual Private Cloud

您的 VPC

子网

路由表

Internet 网关

仅出口 Internet 网关

DHCP 选项集

弹性 IP

终端节点

终端节点服务

NAT 网关

对等连接

安全性

网络 ACL

安全组

VPN 连接

客户网关

虚拟专用网关

VPN 连接

创建路由表 删除路由表 设置为主路由表

搜索路由表及其属性...

	名称	路由表 ID	显式关联与	主路由	VPC
<input checked="" type="checkbox"/>		rtb-c37afcab	0 个子网	是	vpc-af09d8c7   VPC1
<input type="checkbox"/>		rtb-4faa4727	0 个子网	是	vpc-da515cb3

rtb-c37afcab

摘要 路由 子网关联 路由传播 标签

编辑

子网	IPv4 CIDR	IPv6 CIDR
您没有任何子网关联。		
以下子网还没有明确指定与任何路由表关联，所以与主路由表关联:		
子网	IPv4 CIDR	IPv6 CIDR
subnet-3669b75e   subnet1	10.0.1.0/24	-
subnet-536b7828   subnet2	10.0.2.0/24	-

@51CTO博客

两个子网都要关联到路由表中

创建路由表删除路由表设置为主路由表

搜索路由表及其属性...

<input type="checkbox"/>	名称	路由表 ID	显式关联与	主路由	VPC
<input checked="" type="checkbox"/>		rtb-c37afcab	2 个子网	是	vpc-af09d8c7   VPC1
<input type="checkbox"/>		rtb-4faa4727	0 个子网	是	vpc-da515cb3

rtb-c37afcab

摘要

路由

子网关联

路由传播

标签

取消

保存

关联	子网	IPv4 CIDR	IPv6 CIDR	当前路由表
<input checked="" type="checkbox"/>	subnet-3669b75e   subnet1	10.0.1.0/24	-	rtb-c37afcab
<input checked="" type="checkbox"/>	subnet-536b7828   subnet2	10.0.2.0/24	-	rtb-c37afcab

@51CTO博客

添加一条访问外网的路由，如果不加这条路由，则子网内机器无法跟外网通讯，就算机器上绑定了弹性IP也不行

rtb-c37afcab

摘要

路由

子网关联

路由传播

标签

编辑

查看: 所有规则

目标	目标	状态	已传播
10.0.0.0/16	local	活跃的	否
0.0.0.0/0	igw-5219293b	活跃的	否
172.31.0.0/16	pcx-8075e3e9	活跃的	否

@51CTO博客

5、创建EC2实例

在配置实例时，选择VPC1和任意一个子网

1. 选择AMI

2. 选择实例类型

3. 配置实例

4. 添加存储

5. 添加标签

6. 配置安全组

7. 审核

步骤 3: 配置实例详细信息

配置实例以便满足您的需求。您可以从同一 AMI 上启动多个实例，请求竞价型实例以利用其低价优势，向实例分配访问管理角色等等。

实例的数量1启动至 Auto Scaling 组

购买选项请求竞价型实例

网络vpc-af09d8c7 | VPC1新建 VPC

子网subnet-3669b75e | subnet1 | us-east-2a新建子网

251 个可用 IP 地址

自动分配公有 IP使用子网设置 (禁用)

IAM 角色无创建新的 IAM 角色

关闭操作停止

启用终止保护防止意外终止

监控启用 CloudWatch 详细监控将收取额外费用。

租赁共享 - 运行共享硬件实例将对专用租赁收取额外的费用。

T2 无限启用可能收取额外费用

网络接口

设备	网络接口	子网	主要 IP	辅助 IP 地址	IPv6 IP
eth0	新网络接口	subnet-3669b75e	自动分配	添加 IP	

添加设备

@51CTO博客

配置安全组时，选择创建一个新的安全组，然后添加规则

https://blog.51cto.com/zengestudy/2062005

7/11

1. 选择 AMI2. 选择实例类型3. 配置实例4. 添加存储5. 添加标签6. 配置安全组7. 审核

步骤 6: 配置安全组

安全组是一组防火墙规则，用于控制针对您的实例的流量。在此页面上，您可以添加规则来允许到达您的实例的特定流量。例如，如果您希望设置一个 Web 服务器，并允许 Internet 流量到达您的实例，请添加相应的规则来允许不受限制地访问 HTTP 和 HTTPS 端口。您可以选择一个现有的安全组。[了解更多](#) 有关 Amazon EC2 安全组的信息。

分配安全组

创建一个新安全组

选择一个现有的安全组

安全组名称:

launch-wizard-1

描述:

launch-wizard-1 created 2018-01-17T13:07:38.191+08:00

类型	协议	端口范围	来源	描述
SSH	TCP	22	自定义 0.0.0.0/0	例如管理员桌面 SSH

添加规则

警告

设置为 0.0.0.0/0 的源规则允许所有 IP 地址访问您的接口。我们建议将安全组规则设置为仅允许从已知的 IP 地址进行访问。

@51CTO博客

6、EC2实例绑定弹性IP，并测试本地是否能连接EC2实例

启动实例 连接 操作

按标签和属性筛选，或者按关键字搜索

Name	实例 ID	实例类型	可用区	实例状态	状态检查	警报状态	公有 DNS (IPv4)	IPv4 公有 IP
	i-098001355ffa843d2	t2.micro	us-east-2a	running	正在初始化	无		18.218.15.4

@51CTO博客

1. telnet 18.218.15.4 22 (telnet)

Last login: Wed Jan 17 11:45:44 on ttys000  
→ ~ telnet 18.218.15.4 22  
Trying 18.218.15.4...  
Connected to ec2-18-218-15-4.us-east-2.compute.amazonaws.com.  
Escape character is '^['.  
SSH-2.0-OpenSSH\_7.4

@51CTO博客

可以看到，本地是能连上EC2实例的。

二、多个VPC直接如何打通？

多个VPC要打通网络，需要在VPC之间建立对等连接



aws

服务

资源组

★

VPC 控制面板

用 VPC 筛选

Q 选择 VPC

Virtual Private Cloud

您的 VPC

子网

路由表

Internet 网关

仅出口 Internet 网关

DHCP 选项集

弹性 IP

终端节点

终端节点服务

NAT 网关

对等连接

安全性

网络 ACL

安全组

VPN 连接

客户网关

虚拟专用网关

VPN 连接

创建 VPC

操作

Q 搜索 VPC 及其属性...

X

<input type="checkbox"/>	名称	VPC ID	状态	IPv4 CIDR	IPv6 CIDR	DHCP 选项集	路由表	网络 ACL	租赁	默认 VPC
<input type="checkbox"/>		vpc-da515cb3	available	172.31.0.0/16		dopt-4a5d4c23	rtb-4faa4727	acl-e8a5bb81	默认	是
<input type="checkbox"/>	VPC1	vpc-af09d8c7	available	10.0.0.0/16		dopt-4a5d4c23	rtb-c37afcab	acl-3c15bf54	默认	否

选择上面的一个 VPC

@51CTO博客

对等连接名称标签

VPC1\_TO\_DEFAULT

?

选择要用作对等的本地 VPC

VPC (请求方)

vpc-af09d8c7

↕

CIDR

CIDR	状态	状态原因
10.0.0.0/16	● associated	

选择要用作对等的另一个 VPC

账户

● 我的账户

☐ 另一个账户

Region

● This region (us-east-2)

☐ Another Region

VPC (接受方)

vpc-da515cb3

↕

CIDR

CIDR	状态	状态原因
172.31.0.0/16	● associated	

\* 必填

取消

创建对等连接

@51CTO博客

建立对等连接的请求后，一定要记得接收请求，否则不生效

创建对等连接

操作 ^

接受请求

拒绝请求

删除 VPC 对等连接

编辑 DNS 设置

添加/编辑标签

按标签和属性

名称

VPC1\_TO...

状态

正在处理接受

请求者 VPC

vpc-af09d8c7 | VP...

接受方 VPC

vpc-da515cb3

请求方 CIDR

10.0.0.0/16

接受方 CIDR

172.31.0.0/16

请求方所有者

733538584999

接受方所有者

733538584999

@51CTO博客

两个VPC網路的路由上添加路由一条到达对方的路由策略

创建路由表

删除路由表

设置为主路由表

搜索路由表及其属性...

名称

路由表 ID

显式关联与

主路由表

VPC

rtb-c37afcab

2 个子网

是

vpc-af09d8c7 | VPC1

rtb-4faa4727

0 个子网

是

vpc-da515cb3

rtb-c37afcab

摘要

路由

子网关联

路由传播

标签

取消

保存

查看: 所有规则

目标

目标

状态

已传播

删除

10.0.0.0/16

local

活跃的

否

0.0.0.0/0

igw-5219293b

活跃的

否

172.31.0.0/16

否

添加其他路由

igw-5219293b | IGW\_for\_VPC1

pcx-8075e3e9 | VPC1\_TO\_DEFAULT

@51CTO博客

<input type="checkbox"/>	名称	路由表 ID	显式关联与	主路由	VPC
<input type="checkbox"/>		rtb-c37afcab	2 个子网	是	vpc-af09d8c7   VPC1
<input checked="" type="checkbox"/>		rtb-4faa4727	0 个子网	是	vpc-da515cb3

rtb-4faa4727

摘要

路由

子网关联

路由传播

标签

取消

保存

查看: 所有规则

目标	目标	状态	已传播	删除
172.31.0.0/16	local	活跃的	否	
0.0.0.0/0	igw-fd307794	活跃的	否	✕
10.0.0.0/16	pcx-8075e3e9   VPC1_TO_DEFAULT		否	✕

添加其他路由

@51CTO博客

在两个VPC的安全组上添加规则，方形来源是对方IP段的所有流量即可