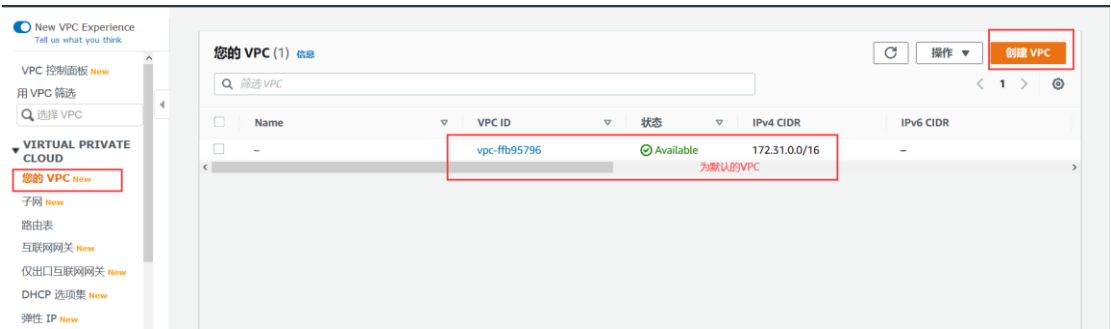


官方文档教程：

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html#VPC_Scenario2_Implementation

一、创建 VPC



VPC 设置

名称标签 - 可选
使用“Name”键和您指定的值创建一个标签。

lab_test_vpc

IPv4 CIDR 块 信息

10.0.0.0/16

IPv6 CIDR 数据块 信息

☒ 无 IPv6 CIDR 块

☐ Amazon 提供的 IPv6 CIDR 块

租期 信息

默认

创建后的 VPC 信息（VPC ID: vpc-029133a194600425f）

VPC > 您的 VPC > vpc-029133a194600425f

vpc-029133a194600425f / lab_test_vpc

操作

详细信息 信息

VPC ID

vpc-029133a194600425f

租期

Default

默认 VPC

否

状态

Available

DHCP 选项集

dopt-9bb658f2

IPv4 CIDR

10.0.0.0/16

DNS 主机名

已禁用

主路由表

rtb-08d9c0c17a6bdf28a

IPv6 CIDR

-

DNS 解析

已启用

主网络 ACL

acl-0d2c02d88b72afc56

所有者 ID

594881697267

创建 Internet 网关：

VPC > 互联网网关 > 创建互联网网关

创建互联网网关 信息

互联网网关是将 VPC 连接到互联网的虚拟路由器。要创建新的互联网网关，请在下方指定网关的名称。

互联网网关设置

名称标签

使用 "Name" 键和您指定的值创建一个标签。

lab_test_internet_gateway

Internet 网关名称

标签 - 可选

标签是分配给 AWS 资源的标记。每个标签都由一个键和一个可选值组成。您可以使用标签来搜索和筛选资源或跟踪 AWS 成本。

键

值 - 可选

Q Name

×

Q lab_test_internet_gateway

×

移除

添加新标签

您可以再添加 49 个 标签。

取消

创建互联网网关

Internet 网关 ID: igw-07ec1d4fe7b2f0275

VPC > 互联网网关 > igw-07ec1d4fe7b2f0275

igw-07ec1d4fe7b2f0275 / lab_test_internet_gateway 操作 ▾

详细信息 信息

互联网网关 ID

igw-07ec1d4fe7b2f0275

状态

Detached

VPC ID

-

所有者

594881697267

标签

管理标签

Q 搜索标签

< 1 > ⚙

Key	Value
Name	lab_test_internet_gateway

将网关附加到 VPC 上

VPC > 互联网网关 > igw-07ec1d4fe7b2f0275

igw-07ec1d4fe7b2f0275 / lab_test_internet_gateway 操作 ▴

详细信息 信息

互联网网关 ID

igw-07ec1d4fe7b2f0275

状态

Detached

VPC ID

-

所有者

594881697267

标签

管理标签

Q 搜索标签

< 1 > ⚙

Key	Value
Name	lab_test_internet_gateway

附加到 VPC

与 VPC 分离

管理标签

删除

VPC > 互联网网关 > 附加到 VPC (igw-07ec1d4fe7b2f0275)

附加到 VPC (igw-07ec1d4fe7b2f0275) 信息

VPC

将互联网网关附加到 VPC 以实现 VPC 与互联网之间的通信。在下方指定您要附加的 VPC。

可用的 VPC

将互联网网关附加到该 VPC。

Q 选择 VPC

vpc-029133a194600425f - lab_test_vpc

▶ AWS 命令行界面命令

取消

连接互联网网关

二、创建公有子网

创建子网 信息

VPC

VPC ID

在此 VPC 中创建子网。

vpc-029133a194600425f (lab_test_vpc)

选择之前自定义的VPC

已关联的 VPC CIDR

IPv4 CIDR

10.0.0.0/16

子网设置

为该子网指定 CIDR 块和可用区。

子网 1, 共 1 个

子网名称

使用“名称”键和您指定的值创建一个标签。

lab_test_subnet_public

名称最多可包含 256 个字符。

子网名称

可用区 信息

选择子网将驻留的区域，或者让 Amazon 为您选择。

无首选项

IPv4 CIDR 块 信息

Q 10.0.0.0/24

▼ 标签 - 可选

键

Q Name

值 - 可选

Q lab_test_subnet_public

移除

添加新标签

您可以再添加 49 个 标签。

子网 ID: subnet-0caea02c7e533defe

subnet-0caea02c7e533defe / lab_test_subnet_public

操作

详细信息

子网 ID subnet-0caea02c7e533defe	状态 Available	VPC vpc-029133a194600425f lab_test_vpc	IPv4 CIDR 10.0.0.0/24
可用 IPv4 地址 251	IPv6 CIDR -	可用区 ap-east-1a	可用区 ID ape1-az1
路由表 rtb-08d9c0c17a6bdf28a	网络 ACL acl-0d2c02d88b72afc56	默认子网 否	自动分配公有 IPv4 地址 否
自动分配 IPv6 地址 否	自动分配客户拥有的 IPv4 地址 否	客户拥有的 IPv4 池 -	Outpost ID -
拥有者 594881697267	子网 ARN arn:aws:ec2:ap-east-1:594881697267:subnet/subnet-0caea02c7e533defe		

新建公有子网路由表（即图中的 Custom route table）：

路由表 > 创建路由表

创建路由表

路由表指定在 VPC、Internet 和 VPN 连接内的子网之间转发数据包的方式。

名称标签lab_test_public_route_table

路由表名称

VPC*vpc-029133a194600425f

按属性筛选

vpc-fb95796

vpc-087407235e570a2f8

vpc-0ed29ecb8e52cc621

vpc-029133a194600425f

zoesimin-vpc

test-vpc

lab_test_vpc

值（最多 255 个字符）

此资源当前无标签

* 必填

取消

创建

公有子网与路由表关联，并设置路由：

子网路由表设置

子网 ID
subnet-0caea02c7e533defe

子网ID

路由表 ID
rtb-0a5b4bb7b3f156c00 (lab_test_public_route_table)

选择刚才新建的路由表

rtb-08d9c0c17a6bdf28a

主路由表

rtb-0a5b4bb7b3f156c00 (lab_test_public_route_table)

已关联

目标	目标	状态	已传播
10.0.0.0/16	local	active	否
0.0.0.0/0	igw		否

添加路由

igw-07ec1d4fe7b2f0275

lab_test_internet_gateway

* 必填

取消

保存路由

路由表: rtb-0a5b4bb7b3f156c00 / lab_test_public_route_table 编辑路由表关联

路由 (2)

Q 筛选路由

目标	目标
10.0.0.0/16	local
0.0.0.0/0	igw-07ec1d4fe7b2f0275

关联之后的效果

目前位置，此公有子网下的 EC2 经过附加公网 IP 后，都可以访问互联网或从互联网访问该实例。

三、创建私有子网（外部不能访问 ec2，但是 ec2 可以访问互联网）

子网设置

为该子网指定 CIDR 块和可用区。

子网 1, 共 1 个

子网名称

使用“名称”键和您指定的值创建一个标签。

lab_test_subnet_private

私有子网名称

名称最多可包含 256 个字符。

可用区 信息

选择子网将驻留的区域，或者让 Amazon 为您选择。

无首选项

IPv4 CIDR 块 信息

Q 10.0.1.0/24

▼ 标签 - 可选

键

Q Name

值 - 可选

Q lab_test_subnet_private

移除

添加新标签

您可以再添加 49 个标签。

由于私有子网，需要通过 NAT 网关访问外部互联网，所有我们需要创建一个 NAT 网关：
（注意：NAT 网关必须附加在上面创建的公有子网中）

创建 NAT 网关 信息

创建 NAT 网关并为其分配弹性 IP 地址。

NAT 网关设置

名称 - 可选

使用“名称”键和您指定的值创建一个标签。

lab_test_net_gateway

NET网关名称

名称最多可包含 256 个字符。

子网

选择要在其中创建 NAT 网关的公有子网。

subnet-0caea02c7e533defe (lab_test_subnet_public)

选择公共子网

弹性 IP 分配 ID 信息

为 NAT 网关分配弹性 IP 地址。

eipalloc-0024b31e86c61ee98

分配IP

分配弹性 IP

net 网关 ID: nat-0b143c43bcd5ad747

VPC > NAT 网关 > nat-0b143c43bcd5ad747

nat-0b143c43bcd5ad747 / lab_test_net_gateway

删除

详细信息 信息

NAT 网关 ID

nat-0b143c43bcd5ad747

私有 IP 地址

10.0.0.22

已创建

2021/03/11 14:36 GMT+8

状态

Pending

网络接口 ID

eni-0d2523da5dd9bea82

已删除

-

状态消息 信息

-

VPC

vpc-029133a194600425f / lab_test_vpc

弹性 IP 地址

-

子网

subnet-0caea02c7e533defe / lab_test_subnet_public

新建私有子网路由表（即图中的 Main route table）：

路由表 > 创建路由表

创建路由表

路由表指定在 VPC、Internet 和 VPN 连接内的子网之间转发数据包的方式。

路由表名称

名称标签

lab_test_private_route_table

VPC*

vpc-029133a194600425f

按属性筛选

vpc-ftb95796

vpc-087407235e570a2f8

vpc-0ed29ecb8e52cc621

vpc-029133a194600425f

zoesimin-vpc

test-vpc

lab_test_vpc

值

(最多 255 个字符)

此资源当前无标签

* 必填

取消 创建

私有子网与路由表关联，并设置路由：

编辑路由表关联 信息

子网路由表设置

子网 ID

subnet-0f97ee5c3a4467e16

私有子网ID

路由表 ID

rtb-078cfa7882685d451 (lab_test_private_route_table)

刚刚创建的路由表

路由表 > 编辑路由

编辑路由

目标	目标	状态	已传播
10.0.0.0/16	local	active	否
0.0.0.0/0	nat-		否

添加路由

nat-0b143c43bcd5ad747

lab_test_net_gateway

* 必填

取消 保存路由

路由表: rtb-078cfa7882685d451 / lab_test_private_route_table

编辑路由表关联

路由 (2)

Q 筛选路由

< 1 > ⚙

目标	目标
10.0.0.0/16	local
0.0.0.0/0	nat-0b143c43bcd5ad747

关联之后的效果

到目前位置，此私有子网下的 EC2 经过 NAT 网关访问互联网，但是从互联网不能访问该实例。

四、为 VPC 设置安全组

一般 EC2 实例会默认使用“default”安全组，并不符合要求，我们要自己创建并配置一个安全组。

VPC > 安全组 > 创建安全组

创建安全组 信息

安全组充当实例的虚拟防火墙，以控制入站和出站流量。要创建新的安全组，请填写以下字段。

基本详细信息

安全组名称 信息

lab_vpc_sg

名称不能在创建后进行编辑。

描述 信息

SG

VPC 信息

vpc-029133a194600425f (lab_test_vpc)

创建完之后，选中安全组，创建如下规则。安全组可以控制流量出入，在本文中，为了方便和日后开发，统一采用粗粒度的设置方式，如果有同学想要更细粒度的管理，请自行配置。（此处可参考顶部连接内的设置）

入站规则 信息

类型 信息

所有流量

协议 信息

全部

端口范围 信息

全部

源 信息

自定义

Q

0.0.0.0/0

×

描述 - 可选 信息

删除

添加规则

出站规则 信息

类型 信息

所有流量

协议 信息

全部

端口范围 信息

全部

目标 信息

自定义

Q

0.0.0.0/0

×

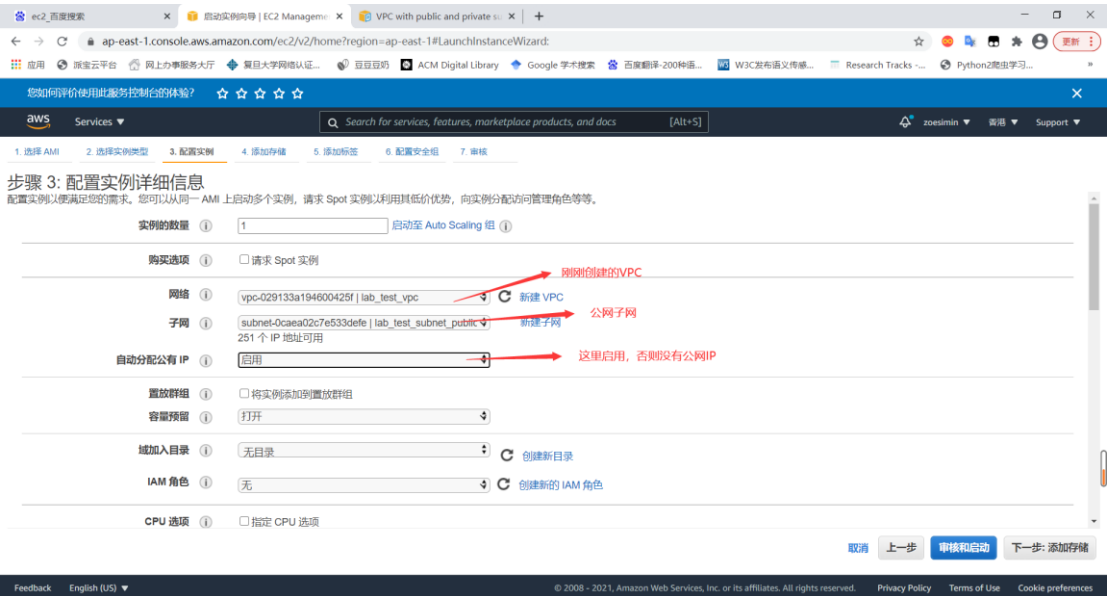
描述 - 可选 信息

删除

添加规则

四、基于自定义 VPC 创建 EC2 实例

分别再启动两个实例，系统选择 **ubuntu18**，分别加入到公网和私网中，公网中的实例要勾选自动分配 IP，如果在这里漏掉，可以在创建完实例之后为其分配弹性 IP。
如下图以公网的配置为例：



步骤 5: 添加标签

标签由一个区分大小写的键值对组成。例如，您可以定义一个键为“Name”且值为“Webserver”的标签。可将标签副本应用于卷和/或实例。

标签将应用于所有实例和卷。有关标记 Amazon EC2 资源的信息，请参阅“[了解更多](#)”。

键 (最多 128 个字符)	值 (最多 256 个字符)	实例 ①	卷 ①	网络接口 ①
Name	lab_test_net_public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

添加其他标签 (最多 50 个标签)

在创建的最后需要创建新的安全组并设置规则。这里给出推荐配置：

公网实例安全组WebServerSG

Inbound Rules

类型	协议	端口	来源
HTTP	TCP	80	0.0.0.0/0
SSH	TCP	22	0.0.0.0/0

Outbound Rules

类型	协议	端口	目的地
所有流量	全部	全部	0.0.0.0/0

私网实例安全组DBServerSG

Inbound Rules

类型	协议	端口	来源
所有流量	全部	全部	10.0.0.0/24

Outbound Rules

类型	协议	端口	目的地
所有流量	全部	全部	0.0.0.0/0

步骤 6: 配置安全组

安全组是一组防火墙规则，用于控制您的实例的流量。在此页面上，您可以添加规则来允许特定流量到达您的实例。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。您可以创建一个新安全组或从下面选择一个现有安全组。有关 Amazon EC2 安全组的信息，请参阅[了解更多](#)。

分配安全组: ☐ 创建一个新的安全组
☒ 选择一个现有的安全组

安全组 ID	名称	描述	操作
sg-099ac314911d72706	default	default VPC security group	复制到新项目
sg-06a40134f96357a88	lab_vpc_sg	SG	复制到新项目
sg-07fcd972d3b90791	launch-wizard-8	launch-wizard-8 created 2021-03-11T14:27:05.967+08:00	复制到新项目

sg-06a40134f96357a88 入站规则 (所选的安全组: sg-06a40134f96357a88)

类型 ①	协议 ①	端口范围 ①	来源 ①	描述 ①
所有流量	全部	全部	0.0.0.0/0	

[取消](#) [上一步](#) [审核和启动](#)

选择现有密钥对或创建新密钥对

密钥对由 AWS 存储的**公有密钥**和您存储的**私有密钥文件**构成。它们共同帮助您安全地连接到您的实例。对于 Windows AMI，需使用私有密钥文件获取登录实例所需的密码。对于 Linux AMI，私有密钥文件让您通过 SSH 安全地登录实例。

注意: 所选的密钥对将添加到为此实例授权的密钥组中。了解更多关于 [从公有 AMI 删除现有密钥对](#) 的信息。

创建新 密钥对

密钥对名称

lab_test_net_publiq

下载密钥对



您必须下载**私有密钥文件**(*.pem 文件)才能继续操作。请将其存储在安全且易于访问的位置。您无法在创建文件后再次下载此文件。

[取消](#)

[启动新实例](#)

启动状态

您的实例正在启动。
以下实例启动操作已开始: i-0b128a42960988180 [查看启动日志](#)

获得预计费用通知
[创建账单警报](#) 以收取电子邮件通知 - 当 AWS 账单预测费用超过设置的值 (例如，您的费用若超过免费套餐)。

如何连接至您的实例

您的实例正在启动，只需几分钟即可进入**运行**状态，到时您就可以使用它了。您的实例上的使用小时数将立即启动并持续统计，直到您停止或终止您的实例。

单击[查看实例](#)监控实例的状态。当您的实例处于**正在运行**状态后，您可以通过“实例”屏幕与之**连接**。有关如何连接至您的实例的信息，请参阅[了解](#)。

这里是一些可帮助您入门的有用资源

- [如何连接至您的 Linux 实例](#)
- [了解 AWS 免费套餐](#)
- [Amazon EC2: 用户指南](#)
- [Amazon EC2: 开发论坛](#)

在实例启动过程中，您还可以

五、与内网实例连接:

与公网实例的连接在 PART1 中“申请服务器”的实验中，同学们已经体验过了，现在要与内网实例连接。

选择通过公网实例连接到内网实例,如果有同学想要直接连接到内网实例,请自行尝试。
把密钥文件传输到公网实例中,先设置密钥权限,然后通过 ssh 命令连接到内网实例。

```
chmod 400 lab_test_net_private.pem
```

```
ssh ubuntu@10.0.1.129 -i ./lab_test_net_private.pem
```

其中 10.0.1.129 是内网实例的私有 IP。

此时内网实例应该能与因特网连通,但是无法被外网访问到,只能通过 VPC 中的公网网段内的实例访问。(如下图所示)

```
ubuntu@ip-10-0-0-177:~$ ls
lab_test_net_private.pem
ubuntu@ip-10-0-0-177:~$ ssh ubuntu@10.0.1.129 -i ./lab_test_net_private.pem
The authenticity of host '10.0.1.129 (10.0.1.129)' can't be established.
ECDSA key fingerprint is SHA256:XeFzuxHY/tVWGXst08z2gkir8+K8l+jg0omyQGaNqJA.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.1.129' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1038-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Thu Mar 11 06:58:31 UTC 2021

System load:  0.0          Processes:            111
Usage of /:   14.6% of 7.69GB Users logged in:      0
Memory usage: 21%         IP address for ens5: 10.0.1.129
Swap usage:   0%

0 packages can be updated.
0 of these updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-1-129:~$ ping www.baidu.com
PING www.wshifen.com (104.193.88.77) 56(84) bytes of data.
64 bytes from 104.193.88.77 (104.193.88.77): icmp_seq=1 ttl=48 time=147 ms
64 bytes from 104.193.88.77 (104.193.88.77): icmp_seq=2 ttl=48 time=147 ms
64 bytes from 104.193.88.77 (104.193.88.77): icmp_seq=3 ttl=48 time=147 ms
^C
```

公网里有私网的密钥文件

跑这个ssh命令
ip地址是私网的那个私有ip

ping的通外网

至此我们完成了 VPC 的配置!