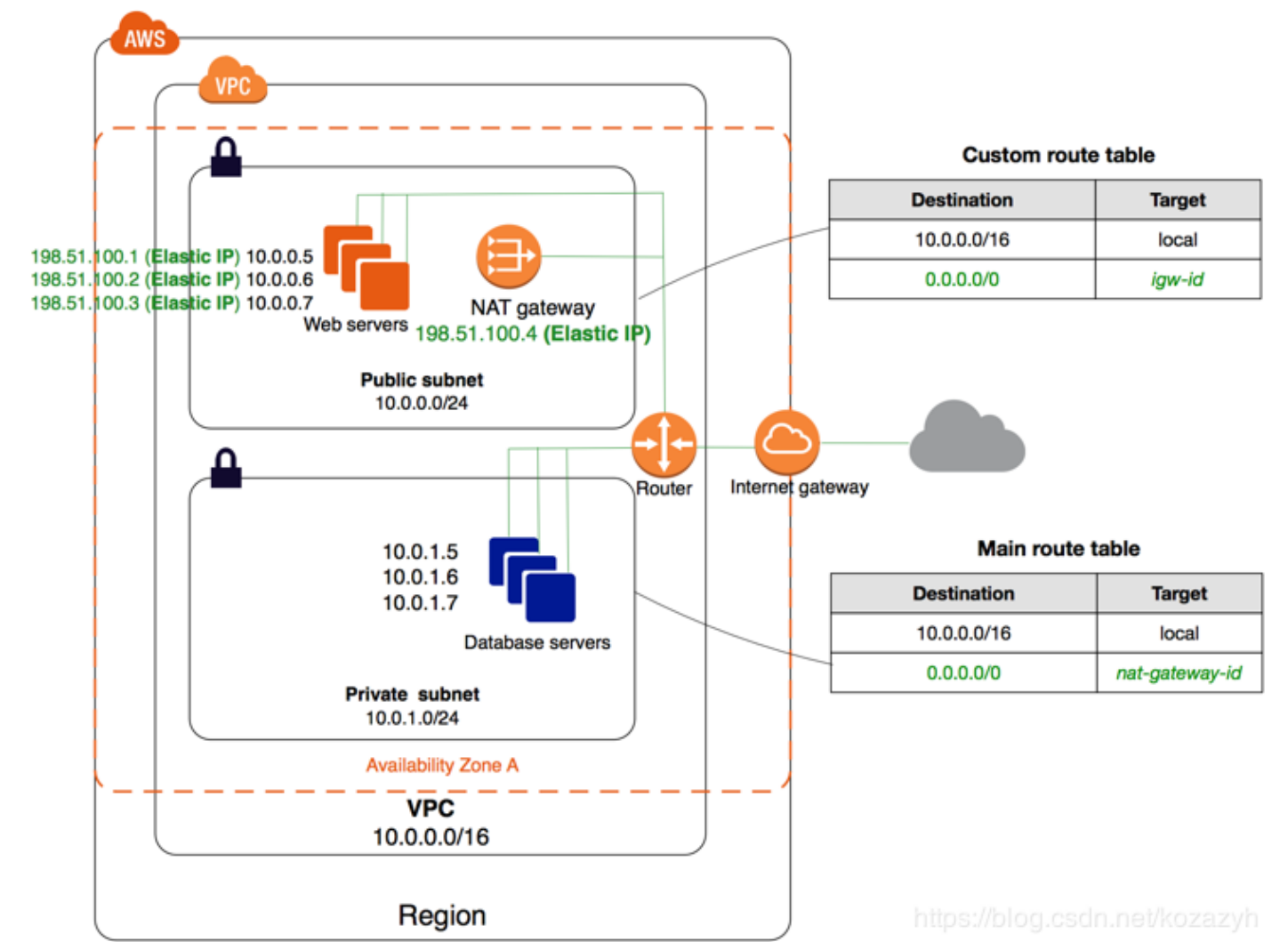


如果您希望运行面向公众的 Web 应用程序，并同时保留不可公开访问的后端服务器，我们建议您配置包括一个有公有子网和私有子网的 Virtual Private Cloud (VPC)。常用例子是一个多层网站，其 Web 服务器位于公有子网之内，数据库服务器则位于私有子网之内。您可以设置安全性和路由，以使 Web 服务器能够与数据库服务器建立通信。

公有子网中的实例可直接将出站流量发往 Internet，而私有子网中的实例不能这样做。但是，私有子网中的实例可使用位于公有子网中的网络地址转换 (NAT) 网关访问 Internet (不建议使用 NAT 实例)。数据库服务器可以使用 NAT 网关连接到 Internet 进行软件更新，但 Internet 不能建立到数据库服务器的连接。

主要组成部分如下图：



注意：NAT gateway必须位于公有子网中，否则流量不能路由到公网。

### 一、创建VPC

aws

服务

资源组

VPC > Create VPC

Create VPC

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You must specify an IPv4 a specify an IPv4 CIDR block larger than /16. You can optionally associate an Amazon-provided IPv6 CIDR block with the VPC.

Name tag

test-vpc

IPv4 CIDR block\*

10.0.0.0/16

IPv6 CIDR block

No IPv6 CIDR Block

Amazon provided IPv6 CIDR block

Tenancy

Default

\* 必填

<https://blog.csdn.net/kozazyh>

创建后的vpc信息 (VPC ID: vpc-04c375aa43719df7b)

VPC: vpc-04c375aa43719df7b

Description

CIDR Blocks

Flow Logs

Tags

VPC ID	vpc-04c375aa43719df7b	Tenancy	default
State	available	Default VPC	No
IPv4 CIDR	10.0.0.0/16	IPv6 CIDR	-
DNS resolution	Enabled	Network ACL	acl-00cdf53db6fcddead9
DNS hostnames	Disabled	DHCP options set	dopt-9ae63ff1
Route table	rtb-0ac65b3236acafd88	Owner	029517931441

<https://blog.csdn.net/kozazyh>

二、创建公有子网

aws

服务

资源组

子网 > 创建子网

创建子网

以 CIDR 格式指定子网的 IP 地址块；例如，10.0.0.0/24。IPv4 块的大小必须介于 /16 网络掩码和 /28 网络掩码之间，可与您的 VPC 大小相同。IPv6 CIDR 块必须是 /64 CIDR 块。

名称标签

test-public

VPC\*

vpc-04c375aa43719df7b

VPC CIDR

CIDR	Status
10.0.0.0/16	associated

可用区域

无首选项

IPv4 CIDR 块\*

10.0.0.0/24

\* 必填

<https://blog.csdn.net/kozazyh>

子网ID: subnet-0fc0ea7528ef94ea9

子网: subnet-0fc0ea7528ef94ea9

描述

流日志

路由表

网络 ACL

标签

Sharing

子网 ID	subnet-0fc0ea7528ef94ea9	状态	available
VPC	vpc-04c375aa43719df7b   test-vpc	IPv4 CIDR	10.0.0.0/24
可用 IPv4 地址	251	IPv6 CIDR	-
可用区域	ap-northeast-2c (apne2-az3)	路由表	rtb-0ac65b3236acafd88
网络 ACL	acl-00cdf53db6fcdead9	默认子网	否
自动分配公有 IPv4 地址	否	自动分配 IPv6 地址	否
Owner	029517931441		

https://blog.csdn.net/kozazyh

创建Internet 网关:

aws

服务

资源组

Internet 网关 > 创建 Internet 网关

创建 Internet 网关

Internet 网关是将 VPC 连接到 Internet 的虚拟路由器。要新建 Internet 网关，请在下方指定网关名称。

名称标签

\* 必填

https://blog.csdn.net/kozazyh

Internet 网关ID: igw-00056fe494c2832d5

Internet 网关: igw-00056fe494c2832d5

描述

标签

ID	igw-00056fe494c2832d5	附加的 VPC ID	-
状态	detached	Owner	029517931441

https://blog.csdn.net/kozazyh

把该网关附加到VPC:

aws

服务

资源组

Internet 网关 > 附加到 VPC

附加到 VPC

为 VPC 附加 Internet 网关，实现 Internet 通信。请在下方指定您要附加的 VPC。

VPC\*

vpc-04c375aa43719df7b

AWS 命令行界面命令

\* 必填

<https://blog.csdn.net/kozazyh>

附加到vpc后,如下:

Internet 网关: igw-00056fe494c2832d5

描述

标签

ID

igw-00056fe494c2832d5

状态

attached

附加的 VPC ID

vpc-04c375aa43719df7b | test-vpc

Owner

029517931441

<https://blog.csdn.net/kozazyh>

修改子网的路由表，增加缺省路由的目的为:internet 网关(igw-00056fe494c2832d5):

Route Table: rtb-0ac65b3236acafd88

Summary

Routes

Subnet Associations

Route Propagation

Tags

Edit routes

View

All routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	igw-00056fe494c2832d5	active	No

<https://blog.csdn.net/kozazyh>

到目前位置，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: subnet-0d20dd3f90894f6e7

描述

流日志

路由表

网络 ACL

标签

Sharing

子网 ID

subnet-0d20dd3f90894f6e7

可用 IPv4 地址

251

可用区域

ap-northeast-2c (apne2-az3)

网络 ACL

acl-00cdf53db6fcddead9

自动分配公有 IPv4 地址

否

Owner

029517931441

状态

available

IPv4 CIDR

10.0.1.0/24

IPv6 CIDR

-

路由表

rtb-0ac65b3236acafd88 | test-public

默认子网

否

自动分配 IPv6 地址

否

<https://blog.csdn.net/kozazyh>

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：

NAT 网关: nat-0c75a0b39681c8b59

详细信息

监控

标签

NAT 网关 ID

状态消息

私有 IP 地址

VPC

创建于

nat-0c75a0b39681c8b59

-

10.0.0.105

vpc-04c375aa43719df7b | test-vpc

2019年4月25日 UTC+8上午10:19:05

状态

弹性 IP 地址

网络接口 ID

子网

已删除

pending

-

eni-0bd44ef68ce7981db

subnet-0fc0ea7528ef94ea9 | test-public

-

<https://blog.csdn.net/kozazyh>

注意：NAT网关必须附加在上面创建的公有子网中

创建私有子网的路由，并配置该路由的缺省路由指向NAT-网关(NAT-Gateway ID: nat-0c75a0b39681c8b59):

Route Table: rtb-0bdd89c77fa558751

Summary

Routes

Subnet Associations

Route Propagation

Tags

Route Table ID

Explicitly Associated with

Owner

rtb-0bdd89c77fa558751

-

029517931441

Main

VPC

No

vpc-04c375aa43719df7b | test-vpc

<https://blog.csdn.net/kozazyh>

Route Table: rtb-0bdd89c77fa558751

Summary

Routes

Subnet Associations

Route Propagation

Tags

Edit routes

View

All routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	nat-0c75a0b39681c8b59	active	No

<https://blog.csdn.net/kozazyh>

修改子网的路由，改为使用上面创建的路由（ROUTE ID: rtb-0bdd89c77fa558751）：

子网: subnet-0d20dd3f90894f6e7

描述

流日志

路由表

网络 ACL

标签

Sharing

修改路由表

路由表: rtb-0bdd89c77fa558751 | test-private

1 到 2, 2

目标	目标
10.0.0.0/16	local
0.0.0.0/0	nat-0c75a0b39681c8b59

<https://blog.csdn.net/kozazyh>

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

参考：[https://docs.aws.amazon.com/zh\\_cn/vpc/latest/userguide/VPC\\_Scenario2.html](https://docs.aws.amazon.com/zh_cn/vpc/latest/userguide/VPC_Scenario2.html)