#4 Task: Create VPC, Public & Private Subnets.

Copyright 2023 - CloudSpikes
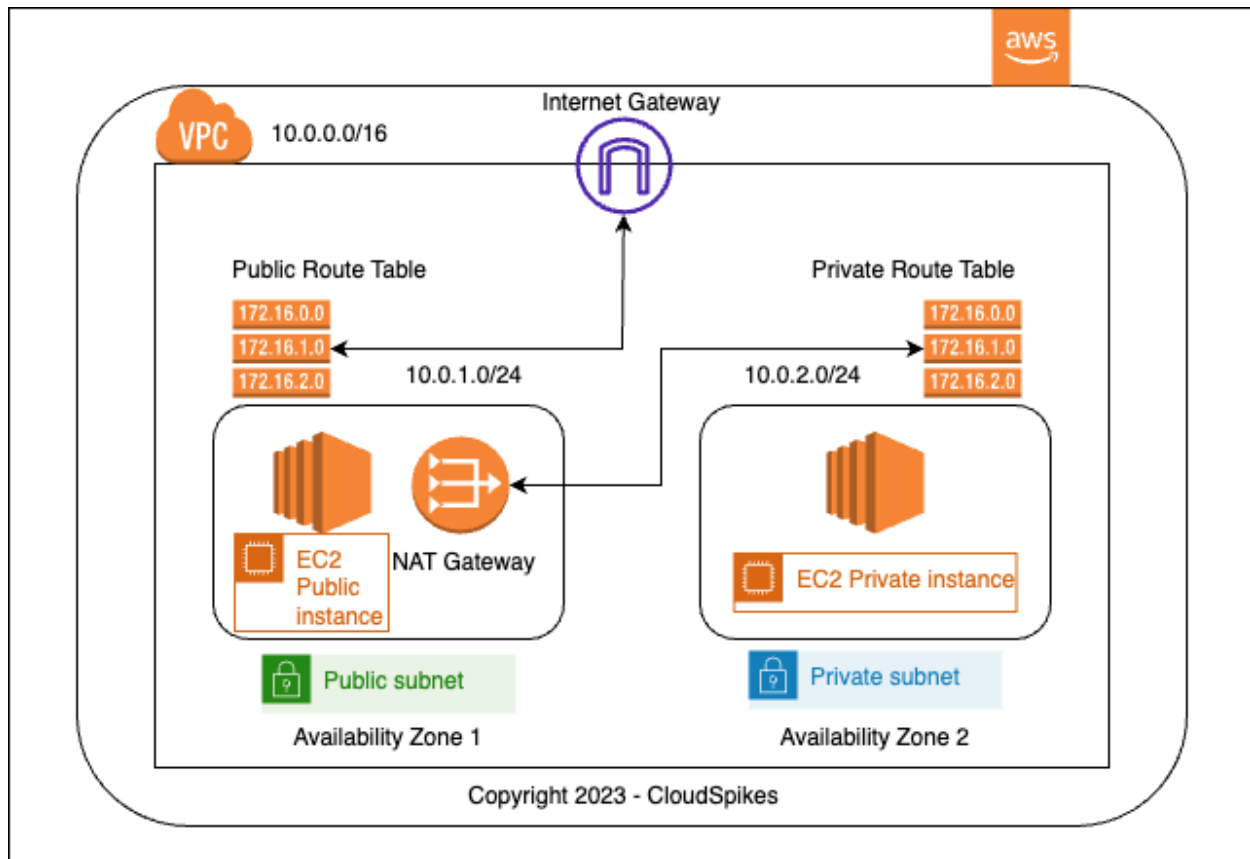
What is a VPC and why is it important?

Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.

Amazon VPC enables you to build a virtual network in the AWS cloud — no VPNs, hardware, or physical data centers required. You can define your own network space, and control how your network and the Amazon EC2 resources inside your network are exposed to the Internet.

What is the importance of having private and public subnets?

The instances in the public subnet can send outbound traffic directly to the internet, whereas the instances in the private subnet can't. Instead, the instances in the private subnet can access the internet by using a network address translation (NAT) gateway that resides in the public subnet.

Requirements:
- AWS Console → https://aws.amazon.com/free/
- Patience…

The Process:
- Follow the steps below. Use the same IPv4 CIDR block numbers. You can make the names of the VPC, subnets, route tables, IGW, NAT gateways unique to whatever you want.

1. Create VPC from VPC Dashboard from AWS Console.

- Click on Create button which will create a VPC

2. Create subnets now, we'll start with creating a public subnet now.

VPC ID is the vpc you created

Availability Zone I left as no preference for this particular project.

3. Let's create a private subnet now.

This can be created using Subnets options from left hand side list in VPC Dashboard. Same process as the public subnet, except we are using a different IPv4 CIDR block.
- Click on create subnet button.

What is an AWS CIDR block?
- When you create a VPC, you must specify a range of IPv4 addresses for the VPC in the form of a Classless Inter-Domain Routing (CIDR) block; for example, 10.0. 0.0/16 . This is the primary CIDR block for your VPC.

4. Modify Auto assign IP by right clicking on public subnet.

5. Create an Internet Gateway to use with our Public Subnet.

Yes, it's really as easy as just creating a tag.

6. Attach Internet Gateway to VPC.
- When you right click on internet gateway, it will show you Attach to VPC option as below.
- Select the VPC you created and click on attach.

7. Create Route Tables.
- A route table contains a set of rules, called routes, that are used to determine where network traffic from your subnet or gateway is directed. To put it simply, a route table tells network packets which way they need to go to get to their destination.

public route table

private route table
- Add Internet Gateway to Public Route Table. Click ADD routes and attach.

8. Edit Subnet Association
- Repeat steps for both your public and private Route Tables.
- Click Edit Subnet Association button.

public route table
private route table

9. Create public and private EC2 instances.
- Follow process for both public and private instances.
- Pay attention to steps for what is particular to a certain instance.

- First step, choose an AMI.

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-04468e03c37242e1e (64-bit x86) / ami-03d381434ef0c36bf (64-bit Arm)

Amazon Linux

Free tier eligible

Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is approaching end of life on December 31, 2020 and has been removed from this wizard.

Root device type: ebs   Virtualization type: hvm   ENA Enabled: Yes

Select

◉ 64-bit (x86)
○ 64-bit (Arm)

- Instance Type.

1. Choose AMI   2. Choose Instance Type   3. Configure Instance   4. Add Storage   5. Add Tags   6. Configure Security Group   7. Review

Step 2: Choose an Instance Type

	Family	Type	vCPUs (i)	Memory (GiB)	Instance Storage (GB) (i)	EBS-Optimized Available (i)	Network Performance (i)
☐	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate
☑	t2	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate
☐	t2	t2.small	1	2	EBS only	-	Low to Moderate

- Public Configure Details

public instance

- Private Configure Details

configure instance details should be the same for both instance, except the public and private subnets.

- Copy and paste User Data from below into PUBLIC instance.

#!/bin/bash
yum install httpd –y
yum update -y
service httpd start
chkconfig httpd on

- Configure Security Group. Make sure to add HTTP port 80 to both public and private instances. SSH port 22 will already be there when created.

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ● Create a **new** security group
○ Select an **existing** security group

Security group name: launch-wizard-15

Description: launch-wizard-15 created 2021-04-02T14:28:44.644+05:30

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ		Description ⓘ	
SSH ▾	TCP	22	Custom ▾	0.0.0.0/0	e.g. SSH for Admin Desktop	✕
HTTP ▾	TCP	80	Custom ▾	0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop	✕

Add Rule

Cancel   Previous   **Review and Launch**

configure security group is the same for both public and private instances

public and private instances should be running as so

- Create a keypair or using an existing keypair.

10. Configure NAT Gateway with it's private route table mapping.

- Create a NAT Gateway in the public subnet*. Ensure you are creating the NAT Gateway in public subnet only.

- Attach an Elastic IP Address* to the NAT Gateway. Now a routing should be added to your private subnet

- Go to private subnet's routing table. Add a route to internet through NAT

- Destination as 0.0.0.0/0 and Target as NAT gateway