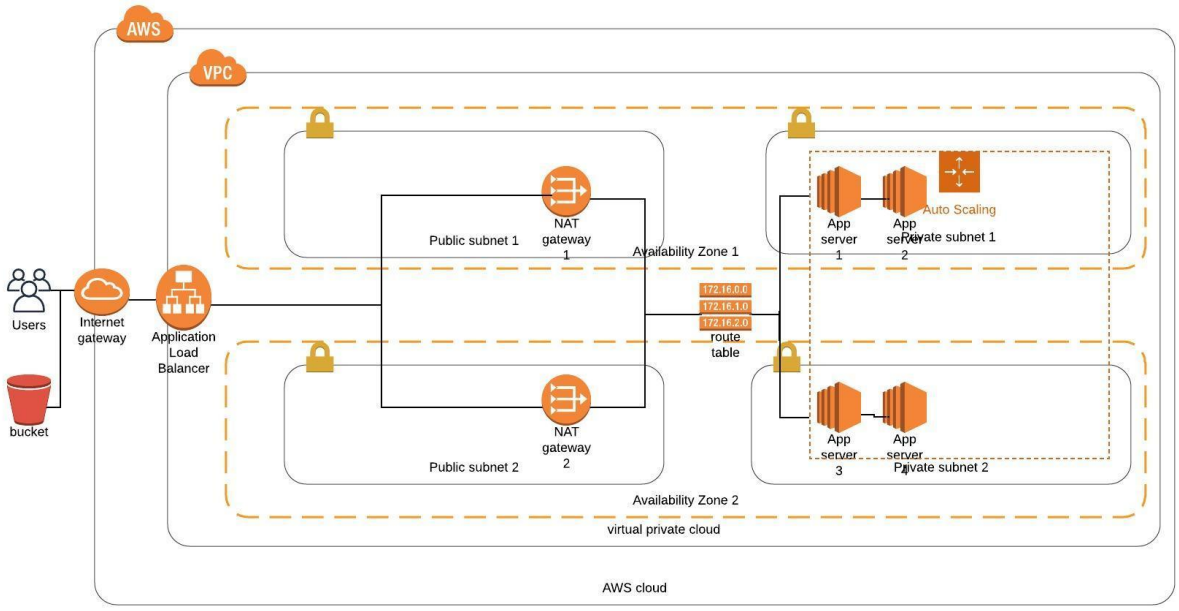
Udacity - Cloud DevOps Engineer

Project 2: Deploy a high-availability web app using CloudFormation

Name: Khoa Nguyen

1. Overview

The following diagram shows the key components of the configuration.



The configuration includes the following:

- A VPC with a size /16 IPv4 CIDR block (example: 10.0.0.0/16). This provides 65,536 private IPv4 addresses.
- An Internet Gateway. This connects the VPC to the Internet and to other AWS services.
- A Load Balancer. It automatically distributes incoming application traffic among multiple targets such as ECS, IPs... and across multiple Available Zones.
- Two public subnets with two size /24 IPv4 CIDR blocks (example: 10.0.0.0/24 and 10.0.1.0/24). Each provides 256 private IPv4 addresses. Two public subnets associated with Internet gateway through Load Balancer.
- Two private subnets with two size /24 IPv4 CIDR blocks (example: 10.0.1.0/24). Each provides 256 private IPv4 addresses.

- Two NAT gateway with their own Elastic IPv4 address. Four Instances in two private subnets can send requests to the Internet through the NAT gateway over IPv4 (for example, for software updates).
- The main route table associated with the private subnet. The route table contains an entry that enables instances in the subnets to communicate with other instances in the VPC over IPv4, and an entry that enables instances in the subnet to communicate with the Internet through the NAT gateway over IPv4.

2. Routing:

All traffic from each subnet that is bound for AWS (for example, to the Amazon EC2 or Amazon S3 endpoints) goes over the Internet gateway. Private subnets can't receive traffic from the Internet directly because they don't have Elastic IP addresses. However, they can send and receive Internet traffic through the NAT devices in the public subnets.

Any additional subnets that you create use the main route table by default, which means that they are private subnets by default.

Main Route Table:

The first entry is the default entry for local routing in the VPC; this entry enables the instances in the VPC to communicate with each other. The second entry sends all other subnet traffic to the NAT gateway (for example, nat-12345678901234567).

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*nat-gateway-id*

3. Security

Security groups control inbound and outbound traffic for the instances.

There are the two following security groups:

- **WebServerSecurityGroup**: Allow http to our host and SSH from local only
- **PublicLoadBalancerSecurityGroup**: Allow http to our load balancer

WebServerSecurityGroup Rule:

Inbound			
Source	**Protocol**	**Port Range**	**Comments**
0.0.0.0/0	TCP	80	Allow inbound HTTP access to the app servers from any IPv4 address.
Your home network's public IPv4 address range	TCP	22	Allow inbound SSH access to Linux instances from your home network.

Outbound			
Source	**Protocol**	**Port Range**	**Comments**
0.0.0.0/0	TCP	0-65535 (All)	Allow outbound traffic to other instances assigned to this security group.

PublicLoadBalancerSecurityGroup Rule:

Inbound			
Source	**Protocol**	**Port Range**	**Comments**
0.0.0.0/0	TCP	80	Allow inbound HTTP access to the web servers from any IPv4 address.

Outbound			
Source	**Protocol**	**Port Range**	**Comments**
0.0.0.0/0	TCP	80	Allow outbound traffic to other instances assigned to this security group.