Index

Solution Summary

Step by Step process of designing

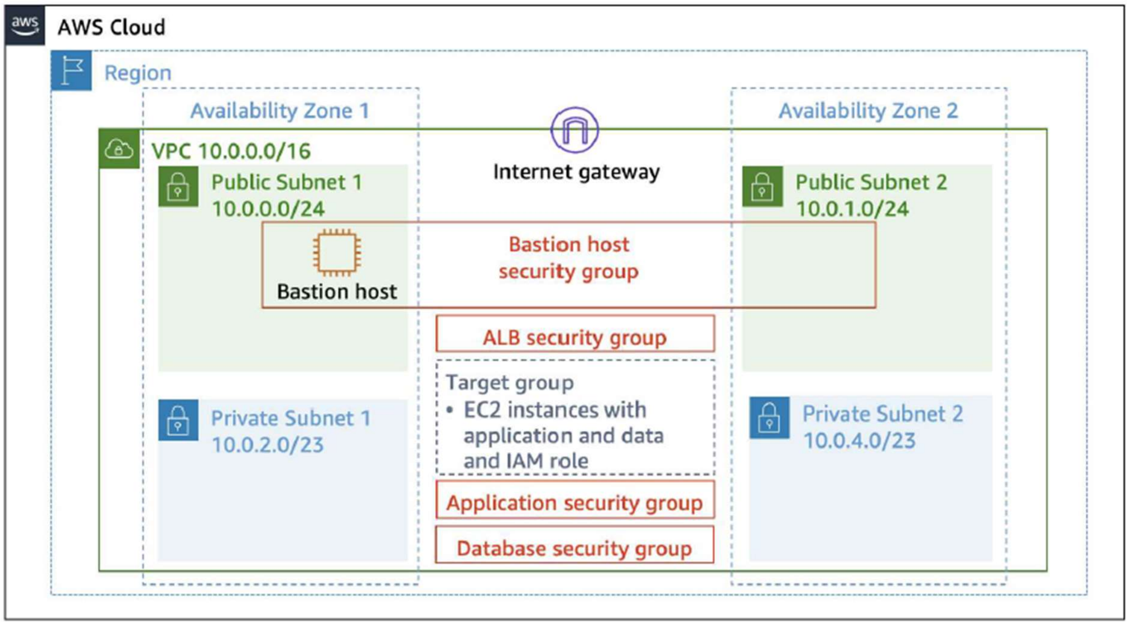
From the initial analysis of the environment, we can understand that we are provided with a VPC “Example VPC”, 4 subnets – “Private subnet 1”, “Private subnet 2”, “Public subnet 1”, and “Public subnet 2”, an internet gateway “Example IGW”. The route table is already connected to “Example VPC” as Public Route Table and Private Route table with 2 subnets each. A total of 4 security groups are also provided which are “Bastion-SG”, “Inventory-App”, “Example-DBSG” and “ALBSG”. In instances, we have one “Bastion” instance running.

Firstly, I created the Application Load Balancer in the “Example VPC” with the mappings done for public subnets. Then I connect it with the Application Load Balancer Security Group (ALBSG) along with a listener. Following the Load balancer, I created the Auto Scaling group with public subnets attached to the created Load Balancer with a max capacity of 2 and desired capacity of 1. This creates another instance. Next, I create a NAT gateway with private subnets and auto-allocated Elastic IP and connect this to private route table 1. Before creating a database, I create a DB subnet group under the “Example VPC” with availability zones of 1a and 1b with private subnets. Now that the DB subnet group is created, I create the database using MySQL being deployed by multi-AZ DB instance with t3.micro storage with 20 GB.

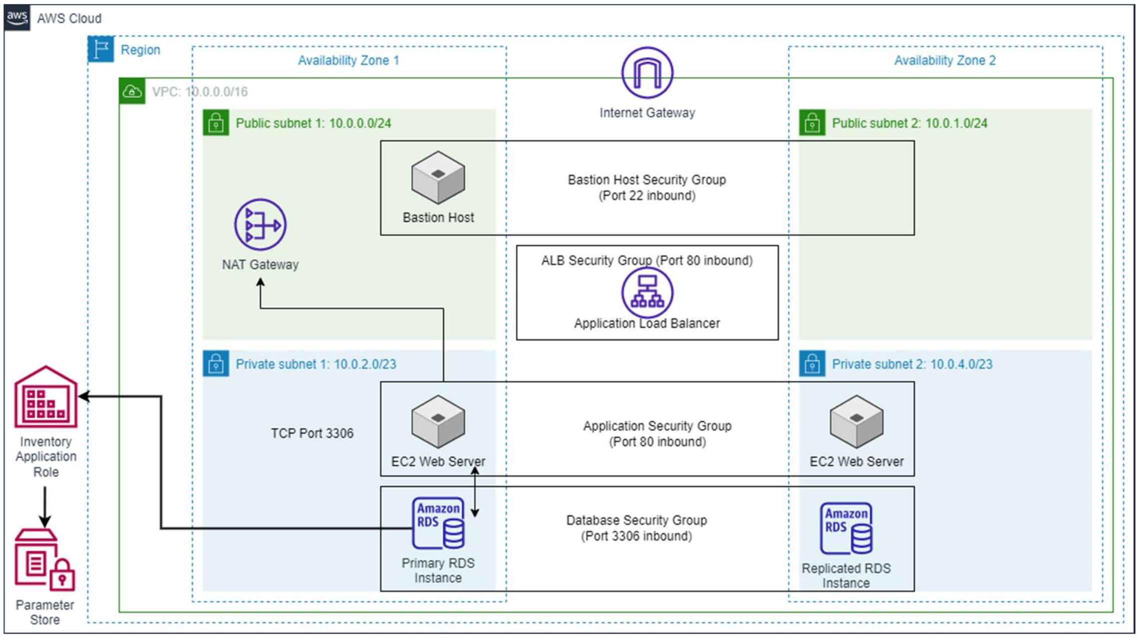
Through the systems manager, I then create parameters. Through the Bastion instance, I connect the private key given to us and connect the web server (instance) created by the Auto Scaling Group. Once this is done, I add the necessary files to the database created earlier. This marks the end of the creation of the cloud architecture. A quick test from the user interface (website) allows us to know if the system is working or not.

Architecture Design

Originally, we are provided with the following architecture:



We are provided with 2 public subnets and 2 private subnets all under the VPC. The VPC is available across 2 availability zones. The public subnet has 1 instance which is the Bastion Host which spans across to the second availability zone through the Bastion Host security group. There are 3 more security groups namely, ALB security group, Application security group and Database security group. The VPC also has an internet gateway which enables us to connect to the Bastion Host through our local system. After working on the received architecture, the following environment was created to support the project.



In the updated environment, we have the AWS cloud which is the entire cloud environment provided by Amazon Web Services. Within the AWS cloud is the AWS region which serves as the physical infrastructure deployment location. This AWS region contains all the resources and services necessary for running applications. The VPC has the IP address of 10.0.0.0/16.

Inside the AWS region resides the VPC (Virtual Private Cloud) which is the virtual network environment where the AWS resources are running. A VPC also allows us to define private network space and control network configurations. Apart from the AWS region, the Availability zones are the data centres deployed inside the region. As seen, there are 2 public subnets, Public Subnet 1 (10.0.0.0/24) and Public Subnet 2 (10.0.1.0/24) which are accessible from the internet. There are also 2 private subnets, Private Subnet 1 (10.0.2.0/23) and Private Subnet 2 (10.0.4.0/23) which are isolated from the internet and provide a secure environment for hosting sensitive resources such as the RDS.

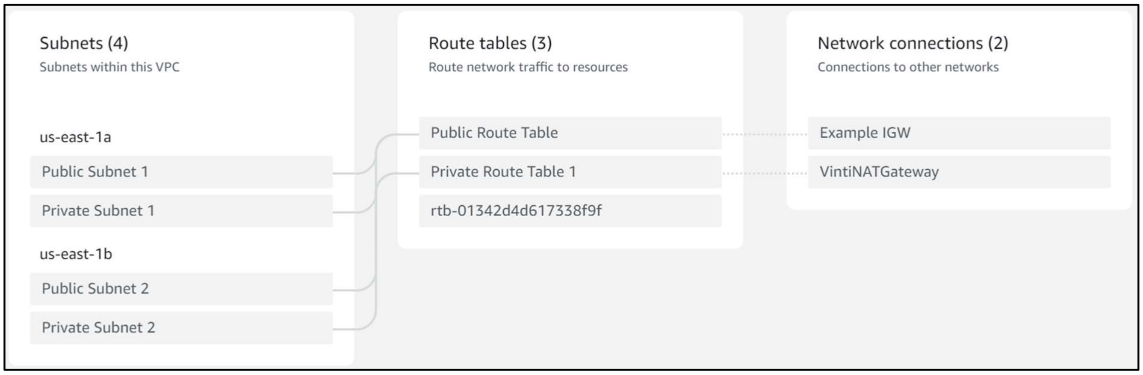
The RDS (Relational Database Service) instances serve as a managed database service in the AWS ecosystem which provides various benefits such as data storage, management, scalability, data security, replication, etc. The replication use case of the RDS instance can be seen in the Private Subnet 2. These RDS instances are governed by the database security group which allows inbound traffic on port 3306 which is the default MySQL port.

The bastion host is the instance in Public Subnet 1 which acts as a secure entry point for accessing resources within the private subnets. The security group, Bastion Security Group defines the inbound rule allowing SSH (port 22) traffic. The EC2 web servers is associated with the Application security group which allows inbound traffic on port 80 (HTTP). These web servers are placed in the Private subnet as requested in the project specifications. The Application Load Balancer Security group is associated with the Application Load Balancer which balances the incoming application traffic between the EC2 web server instances.

There are other components as well such as the Internet gateway which signifies that the resources within the VPC have access to the internet. Along with which is the NAT gateway which allows instances within private subnets to access the internet while keeping them hidden from the external sources. There is also the Inventory Application Role which serves as a role or service responsible for inventory related functionality. Another one is the parameter store which is connected to the Inventory Application using an arrow which means that the Application role interacts with and retrieves configuration or parameter data from the Parameter store.

Based on the connections present in the architecture, we can see that the Primary RDS instance in Private Subnet 1 is connected to the EC2 web server in Public Subnet 1 using a 2-sided arrow which indicates a bi-directional relationship, meaning that the web server can interact with the database and vice-versa. The primary RDS instance in Private subnet 1 is also connected to the Inventory Application Role using an arrow which signifies a uni-directional relationship from the RDS instance to the application role. Lastly, we have the Inventory application role connected to the Parameter store using an arrow signifying another uni-directional relationship.

The resource map for the new Cloud Architecture is given below:



Subnets (4)
Subnets within this VPC

us-east-1a
Public Subnet 1
Private Subnet 1

us-east-1b
Public Subnet 2
Private Subnet 2

Route tables (3)
Route network traffic to resources

Public Route Table
Private Route Table 1
rtb-01342d4d617338f9f

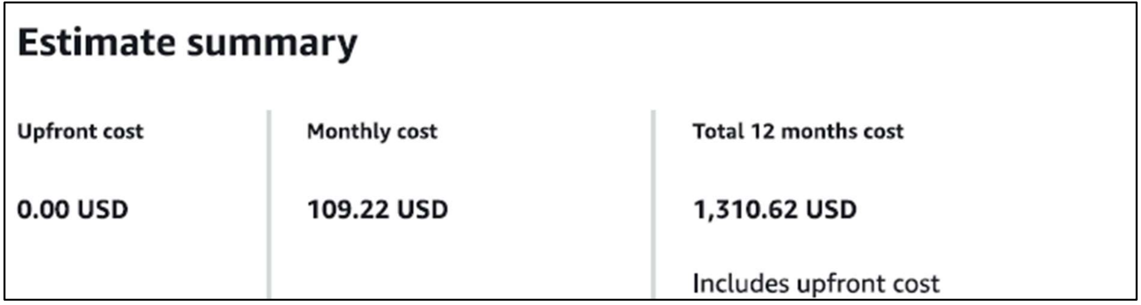
Network connections (2)
Connections to other networks

Example IGW
VintiNATGateway

According to the above resource map, the public subnets are connected to the public route table which determines the next hop for outgoing traffic which in turn is connected to the Internet gateway which means that it uses the Example Internet IGW as the next hop for outbound internet-bound traffic. The private subnets ae connected to the private route table for routing purposes and further connected to the NAT gateway. Overall, the public route table being connected to the Internet gateway enables internet connectivity for resources within the associated public subnets. The private route table on the other hand allows communication among resources within the VPC while keeping the isolated from the internet.

Cost Estimation

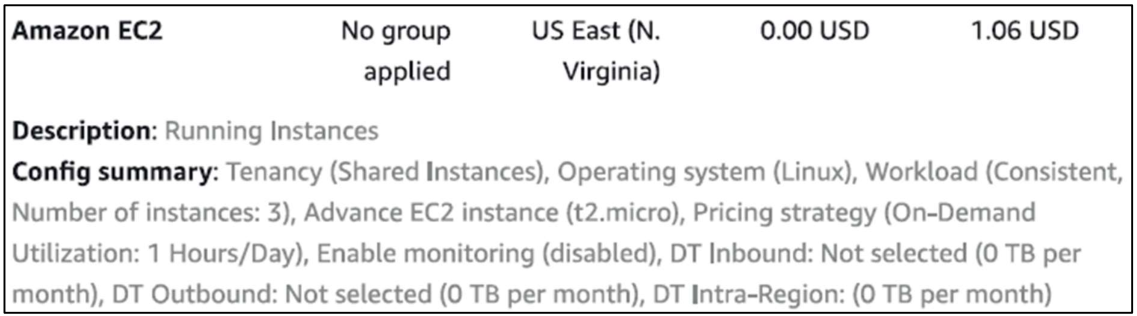
Estimation of Costs
Using the AWS pricing calculator, the following estimate was obtained:



Estimate summary

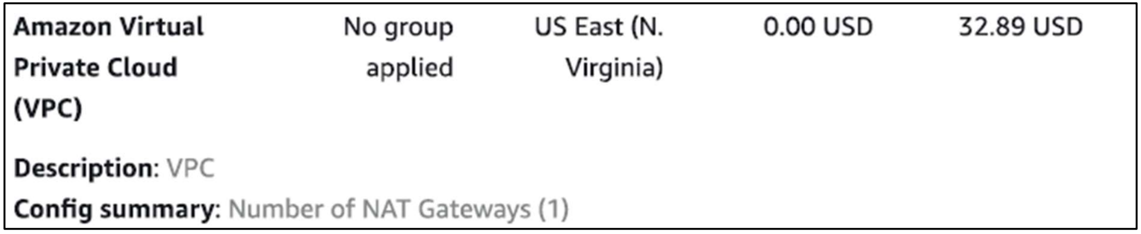
Upfront cost	Monthly cost	Total 12 months cost
0.00 USD	109.22 USD	1,310.62 USD Includes upfront cost

This estimate was obtained through a total of 4 components:



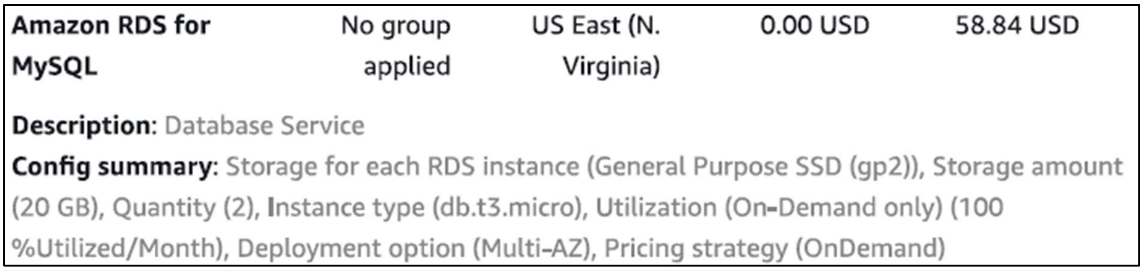
Amazon EC2	No group applied	US East (N. Virginia)	0.00 USD	1.06 USD

Description: Running Instances
Config summary: Tenancy (Shared Instances), Operating system (Linux), Workload (Consistent, Number of instances: 3), Advance EC2 instance (t2.micro), Pricing strategy (On-Demand Utilization: 1 Hours/Day), Enable monitoring (disabled), DT Inbound: Not selected (0 TB per month), DT Outbound: Not selected (0 TB per month), DT Intra-Region: (0 TB per month)



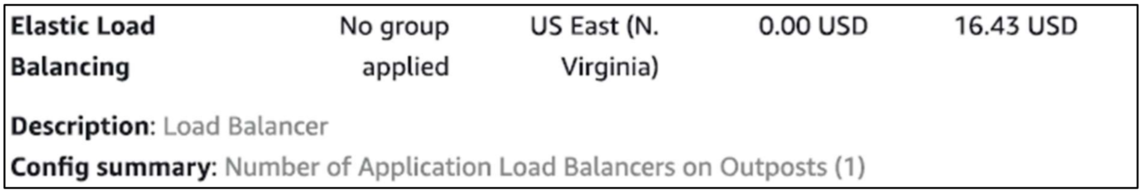
Amazon Virtual Private Cloud (VPC)	No group applied	US East (N. Virginia)	0.00 USD	32.89 USD

Description: VPC
Config summary: Number of NAT Gateways (1)



Amazon RDS for MySQL	No group applied	US East (N. Virginia)	0.00 USD	58.84 USD

Description: Database Service
Config summary: Storage for each RDS instance (General Purpose SSD (gp2)), Storage amount (20 GB), Quantity (2), Instance type (db.t3.micro), Utilization (On-Demand only) (100 %Utilized/Month), Deployment option (Multi-AZ), Pricing strategy (OnDemand)



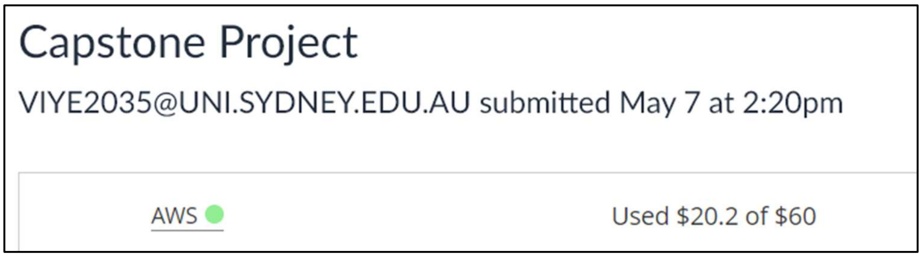
Elastic Load Balancing	No group applied	US East (N. Virginia)	0.00 USD	16.43 USD

Description: Load Balancer
Config summary: Number of Application Load Balancers on Outposts (1)

The above resources were used to estimate an average cost of the overall architecture at base plan. The cost would increase based on the amount of traffic and any other services if required. Based on the monthly costs, we can deduce the estimated daily costs:

$$\frac{Monthly\ cost}{30} = \frac{109.22}{30} = US\$3.64/day$$

Actual Costs



Capstone Project

VIYE2035@UNI.SYDNEY.EDU.AU submitted May 7 at 2:20pm

AWS ●

Used $20.2 of $60

Based on the actual costs incurred through the set up on cloud. We can estimate the following costs:

$$Date\ of\ actual\ cost\ estimation: May\ 18, 2023$$
$$Number\ of\ days\ elapsed: 11$$
$$Daily\ cost = \frac{20.2}{11} = US\$1.84/day$$

Financial Discussion

Based on the calculation of costs, there is a difference of US$1.80/day which would lead to a difference of US$54 over a month and to almost US$650 over a year. This amount of difference is within acceptable range for a website of a huge Non-Profit Organisation. Another thing to note is that this cost might increase on addition of additional services which are not covered by this project as of now.

The security features along with the high scalability of the platform for the incoming traffic would be a good addition to the service provided by the website created by Shirley Rodriguez.

Demonstration Plan

Video Contents

As part of the assignment, the following is the breakdown of the video submitted:

Time Start	Time End	Topic	Description
00:00:00	00:00:25	Intro	Briefly introduced myself and showed my Photo ID.
00:00:25	00:01:41	Q1	Inspected the VPC, the subnets, explained their purposes and their network access permissions.
00:01:41	00:03:44	Q2	Inspected all security groups and explained their purpose and rules.
00:03:44	00:05:45	Q3	Showed admin user and their power to modify databases.
00:05:45	00:06:15	Q5	Shows that website runs on t2.micro EC2 instance and instances are in the private subnet.
00:06:15	00:07:25	Q4	Inspected all running EC2 instances and explained their uses.
00:07:25	00:09:06	Q6	Shows that we can access EC2 instances via the bastion host.
00:09:06	00:09:38	Q7	Inspects the Auto Scaling Group.