Cloud Foundations (AWS)

Project: Version B

Name: Shakeel Schieman

Student Number: EDUV4777433

Date: 6 November 2024

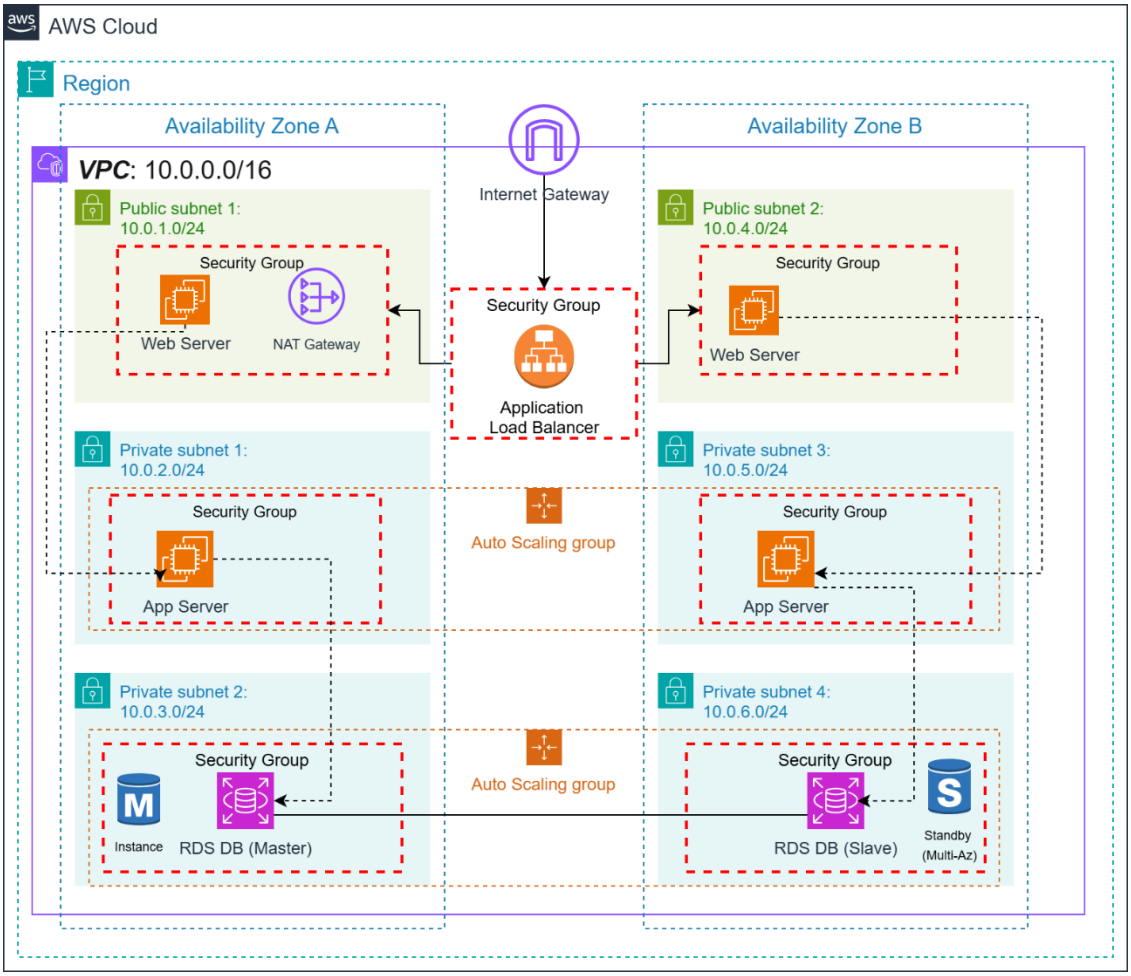

Figure 1AWS Architecture

In this project, the image above illustrates a highly available, secure three-tier architecture in AWS. The architecture ensures high level security and cost effective.

The components that I used is the VPC along with the CIDR range of 10.0.0.0/16, divided in multiple subnets spanning across two availability zones

The architecture shows a three-tier architecture distributed across two availability zones (Availability Zone A and B). In these availability zones we have different layers, a web layer, app layer and database layer. The web layer hosts web servers in public subnets 1 and 2 which are accessible to the internet via an internet gateway. The app layer hosts application servers in private subnets 1 and 3 which are isolated from the internet. In the last layer, database layer it contains a primary RDS database instance in private subnet 2, availability zone A. In private subnet 4, availability zone B there is a secondary RDS database which serves as a replica.

The reason behind using 2 Availability Zones is to ensure high availability and fault tolerance in the infrastructure because by distributing the services across two availability zones, if one service in any availability zone fails, it can be used by the other healthy service in the other availability zone.

In the diagram you can see the Application Load Balancer connected to both the Web Servers which distributes incoming traffic and ensures load distribution and redundancy.

The Auto Scaling Groups surrounding both application servers and RDS databases are there to automatically adjust the number of instances. It optimizes resource usage, and it is cost effective.

The NAT Gateway is there in the public subnet 1 which allows instances in the private subnet to receive internet access for updates and installing patches

Below explains the port numbers for the different security groups

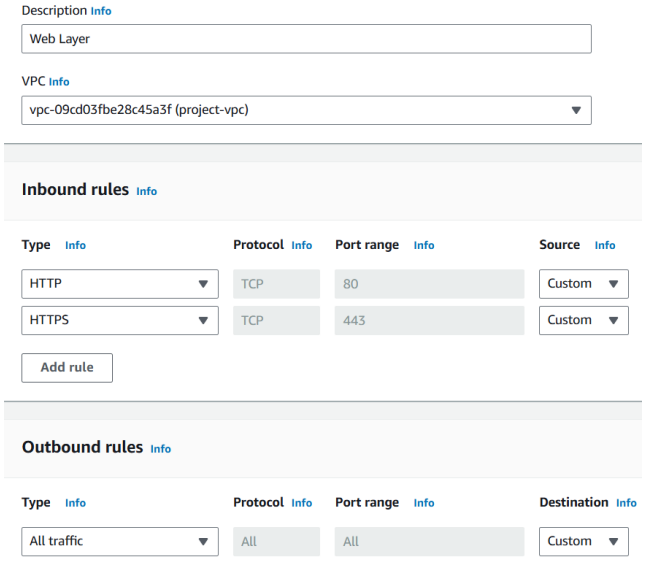

Figure 2 Web Layer Security Group

For the web layer security group, the inbound rules are port 80 for http and port 443 for https which allows inbound http and https traffic from the internet (0.0.0.0/0).

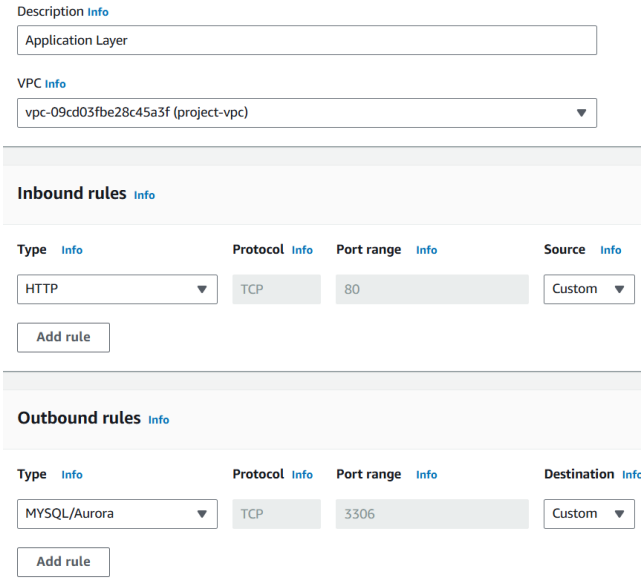

Figure 3 Application Layer Security Group

For the application layer, the inbound rules are port 80 for http which allows traffic only from the web server security group. The outbound rules are port 3306 for MYSQL/Aurora that allows outbound traffic to the database layer.

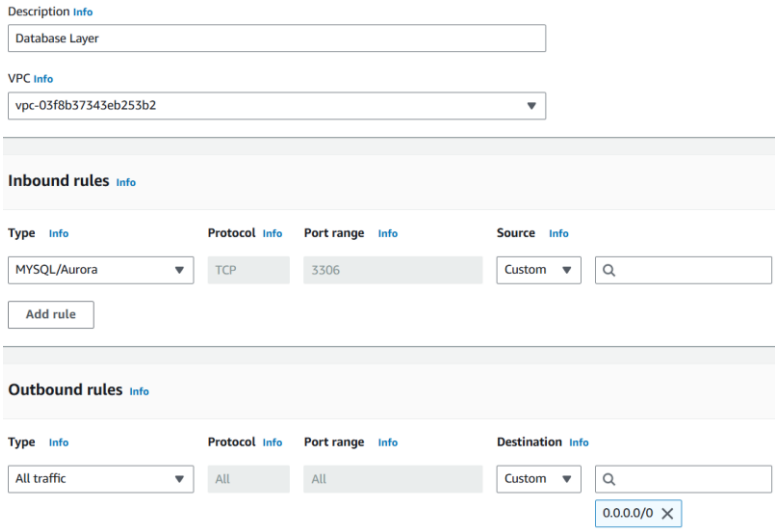

Figure 4 Database Layer Security Group

For the database layer, the inbound rules are port 3306 for MYSQL/Aurora that allows inbound traffic from the application layer.

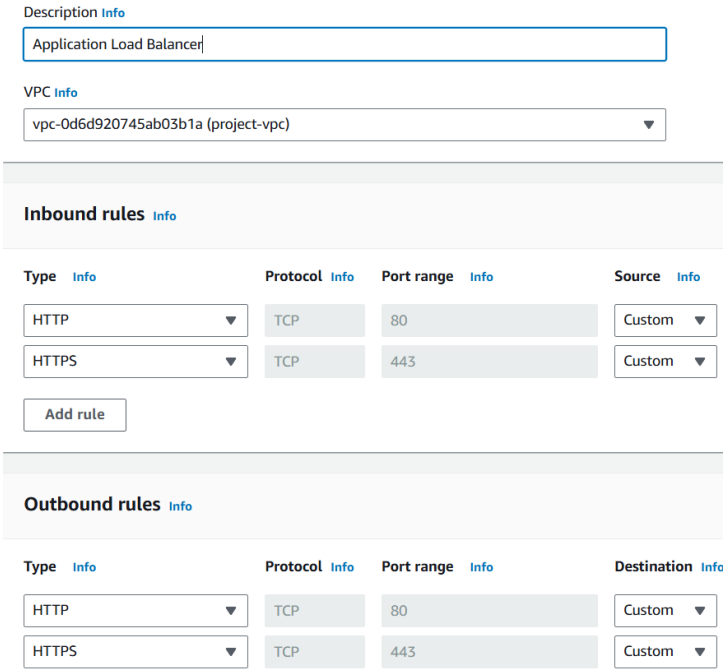

Figure 5 Application Load Balancer Security Group

Application Load Balancer Security Group with Inbound rules for http and https, port 80 and 443 which allows public access that makes it accessible over the internet. Outbound rules are the same, but it sends traffic to the web servers in the public subnets.