

Amazon Web Services

Project overview

This project provides the solution design skills.

Tasks:

Deploy a PHP application that runs on an Amazon Elastic Compute Cloud (Amazon EC2) instance .

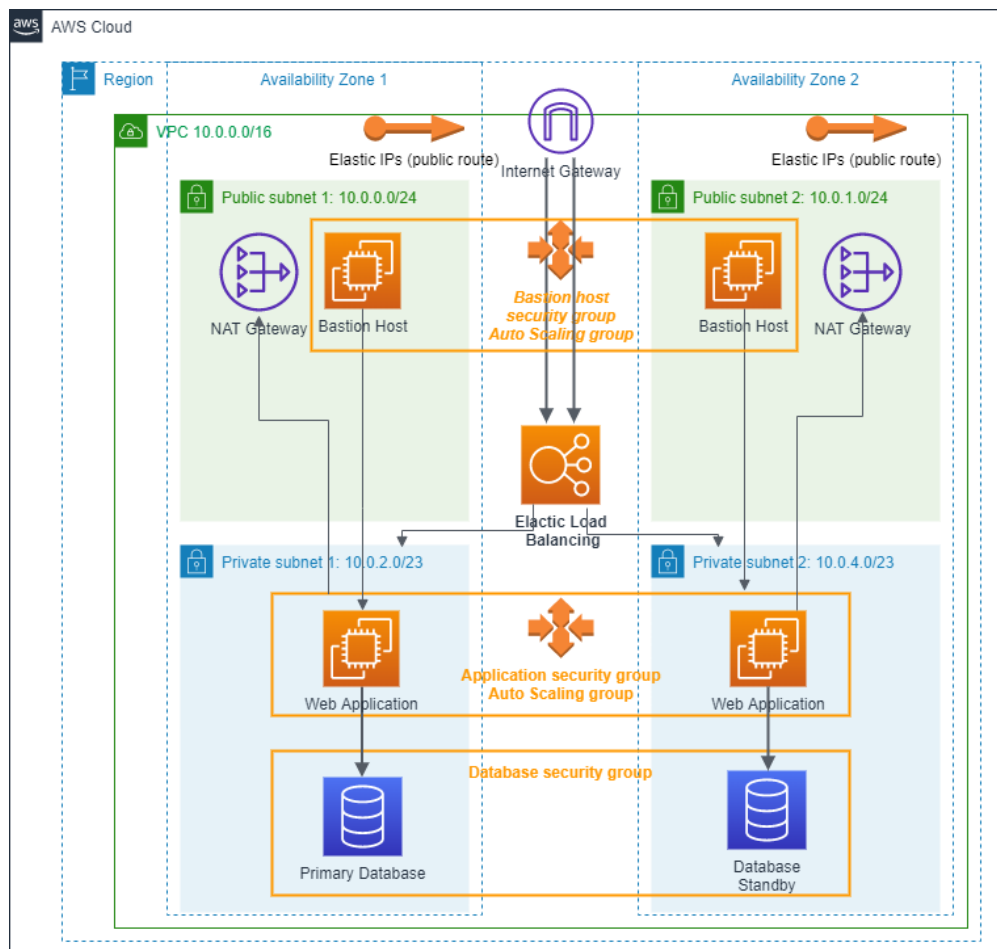
Create a database instance that the PHP application can query.

Create a MySQL database from a structured query language (SQL) dump file .

Update application parameters in an AWS Systems Manager Parameter Store .

Secure the application to prevent public access to backend systems.

A diagram of the solution.



High Availability

Two NAT gateways in each public subnet. The bastion hosts are deployed on Auto Scaling Group (the maximum instances of 1 in each subnet).

The WEB application servers and databases are deployed in private subnets.

In such an architecture, the high availability of the whole system can be achieved.

The replication of the web application server allows workload distribution across multiple application services.

The standby database was connected to the main database.

Security

The Bastion host machines have a security group rule, which allows connection by SSH from the internet. The Web application servers are isolated in the private subnets and protected by a security group with the rule of allowing SSH connection from bastion host, and HTTP/HTTPS traffic from Elastic Load Balancer.

The database instances are also covered by a separate security group which allows only SQL connections from Web Application instances (port 3306).

Deployment

The deploying process begins by creating the Key Pair.

Then by creating a stack by Cloud Formation for bastion hosts, the maximum running instance in each public subnet will be 1.

The second step was to deploy the web application servers in each private subnet, again the Cloud Formation tool was used for that, and a webpage template was used to deploy a webpage on them.

In the next step, two database instances in private subnets were deployed, and both have been protected by security rules to allow traffic from web application servers to the database using port 3306. The NAT gateways were added to the public subnets to make web application servers available to communicate with the internet.

After that, the database dump was uploaded to deploy the database instances. Also, the following parameters had been added to the parameter store, so the web application server can use it to connect to the database.

/example/endpoint

/example/username

/example/password

/example/database

The Multi-AZ deployment was used for database instances.