CSCI4145/5409: Network & Security

Reminder: This is an individual assignment. You are not allowed to collaborate with anyone else when completing this assignment. You can borrow code and configuration snippets from internet sources that are not from students in this class, however that code must be cited and include comments for how you have modified the original code.

Introduction

This assignment will measure your understanding of some of the network and security mechanisms of our cloud provider AWS. This assignment assures us that you have attended the tutorials and learned about AWS VPC, RDS and Secrets Manager, or that you have found some other way to learn these services.

Learning Outcomes

- Learn the importance and role of Virtual Private Clouds in creating secure architectures that maximize the principle of least privilege (i.e. if a server does not need to be publicly reachable or have its traffic go across the Internet, then it should be behind some protective measure)
- Learn how to implement a VPC on AWS
- Apply your learning by implementing one **public** facing service inside the VPC that is accessible to the public internet
- Apply your learning by implementing one **private** service inside the VPC that is **not** accessible to the public internet, used by the public facing service
- Learn to apply AWS security practices by using Secrets Manager to store private information
- More experience working with AWS libraries that allow you to perform AWS operations
- More experience building REST APIs, and working with arrays in JSON

By now you have all learned that cloud computing can be tricky and complicated. You have learned that provisioning IT resources correctly is complicated, and a small mistake can lead to hours of debugging and searching for answers. I **highly** recommend that you start this assignment early, and that you follow my tutorial so that you understand how to properly provision everything. There is a link at the end of this document that is the AWS tutorial that I followed in our tutorial on March 7th in Collaborate Ultra. **This architecture will be too complex for me to debug with you individually if you make mistakes. Proceed carefully and meticulously.**

Requirements

You will build a web application with any language or framework you like, **deployed on an EC2 instance behind a Virtual Private Cloud (VPC)**.

Your application running on EC2 will be public facing (accessible through a Public IP you assign to it on launch, or an elastic IP you create for it), and listening to **POST** requests to /storestudents, and **GET** requests to /liststudents.

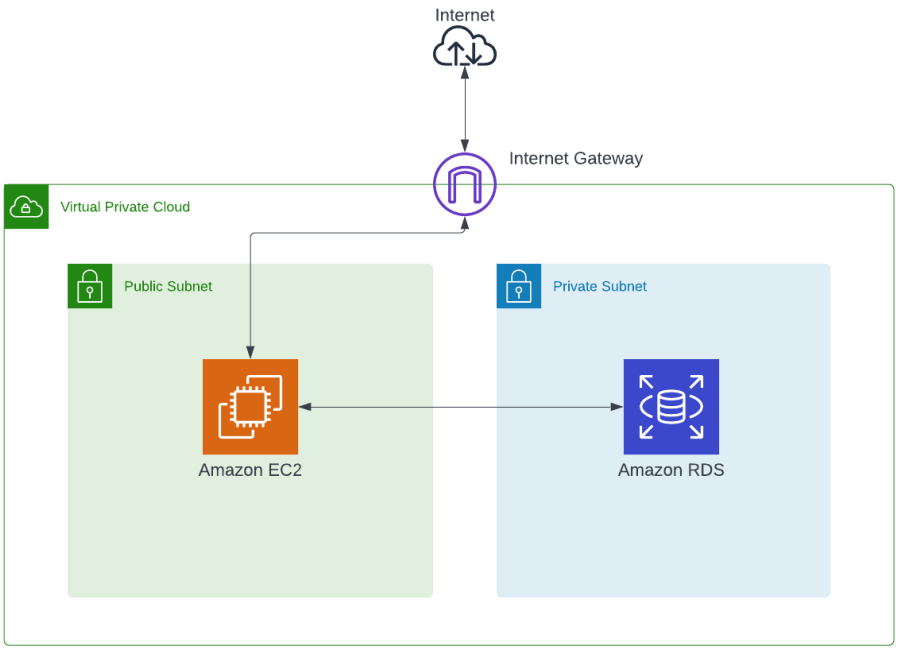
/storestudents will:

- Receive and parse a JSON body
- Connect to an AWS RDS database server running on a private subnet inside your VPC
- Insert one record into the **students** table in the database *for each item* in the students array in the JSON body
- Return a status 200 code if everything works, or 400 and an error message if there is a failure

/liststudents will:

- Connect to the AWS RDS database running on the private subnet inside your VPC
- Query the **students** table and return a list of all students to display in a browser. How you display the student information is up to you, but it must be legible.

When you are finished the system will look and function like this:



Additonal Requirement – Secrets Manager

To connect to your RDS database you will need a **username** and **password.** Store this information in Secrets Manager, and retrieve it from Secrets Manager in your code using your access key, secret access key and session token credentials from your lab environment.

Your RDS database:

You may choose whichever type of database you are comfortable with; I recommend Aurora because this database is covered in the tutorial. I do not recommend SQL Server or Oracle as these DBs will devour your credits.

Your database must contain a single table named **students** that has the following schema:

```
CREATE TABLE students (
     first_name varchar(100),
     last_name varchar(100),
     banner varchar(20)
)
```

JSON You Will Send Your App

Your app will receive the following JSON input to the /storestudents endpoint:

```
{
   "students": [
      {
         "first_name": "<a name>",
         "last_name": "<another name>",
         "banner": "<banner #>"
      },
      {
         "first_name": "<yet another name>",
         "last_name": "<yet another name>",
         "banner": "<another banner #>"
      },
      ...
   ]
}
```

Note the following:

- <>'s are placeholders intended to mean you replace this with some other text
- … indicates that the "students" object is an array that can have any length, including being empty!

How To Submit

Submit the following to the assignment drop box on Brightspace:

- A video you record doing the following:
    - Using postman (or a similar tool) to **POST** some students to your EC2 server's /storestudents endpoint from your computer (not from the EC2 server itself, this demonstrates that you have set up your VPC correctly)
    - Use the AWS console to load up your VPC and show your public and private subnets, go slow so we can see things clearly. Show any security groups, elastic IPs and subnets you have created.
    - **Show your Secrets Manager configuration and where your username and password for the RDS database are saved, also show how these values are retrieved in your code and used to connect to your database.**
    - Show your RDS config, demonstrate that it is running inside your private subnet
    - Use a browser to load your /liststudents endpoint and demonstrate that your code properly returns all of the student information you passed to /storestudents earlier. Make sure these match so that we can verify that you aren't just returning hardcoded values.
- Your code in a zip file so that we can perform an AIO check

Your TAs will review your videos and assign your grade. Make their job easy by verifying that your video has everything clearly visible and legible. **If they can't see something, they aren't going to assume it works, they will give you a zero for that item.**

Marking Rubric

Your submission will be marked by the TAs reviewing your videos:

- **Your VPC configuration is correct: 40%**
    - **There is a private subnet (or multiple private subnets if RDS requires it)**
    - **There is a public subnet**
    - **The EC2 server is in the public subnet**
    - **RDS is in the private subnet(s)**
- **Your app uses Secrets Manager to store the username and password for your RDS database, which you retrieve programmatically using your AWS Academy lab credentials – 10%**
- **Your app properly parses the incoming JSON to /storestudents and stores the information in the students table in RDS – 25%**
- **Your app properly queries the RDS students table and displays a list of students in the database from the /liststudents endpoint – 25%**

AWS Tutorial

This tutorial will be very helpful in your preparation of the assignment. You can watch me progressing through this tutorial by reviewing the Network tutorial on Collaborate Ultra:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Tutorials.WebServerDB.CreateVPC.html