**Group Project Name: Cloud Security**

**Technology: AWS Public Cloud**

**Student: Gagneet S.**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Intended Services / Technologies to Provision:**

EC2 Instances

IAM Roles

Security Groups

VPCs

Subnets

Regions

Availability Zones

**Design:**

Research Security for the Public Cloud

Define the terms indicated

Use your understanding of these concepts to architect a robust security profile / infrastructure as detailed below.

**Important Note:**

When you are designing and deploying services, documentation can be of great help as replicating exact configurations can at times be challenging. Note: When we do not replicate a configuration exactly, we can end up creating security issues (assuming we had a “secure” or robust design initially). Another reason to develop good documentation is that it gives a good idea of what should be happening with systems and it can be reviewed and refined over time so that the quality of your designs and configurations increases as you practice.

**Terminology to Define:**

“Shared Responsibility” Model

“Lift and Shift” Migration and the Resulting Security Implication

(from on premise to the public cloud)

Regions (AWS)

Availability Zones (AWS)

Security Groups (AWS)

VPCs (AWS)

Subnets (AWS)

IAM Roles (AWS)

**Questions to Answer:**

**Security (Overall):**

Explain (in detail) the concept of the “Shared Responsibility” model in the Public Cloud? Give examples of aspects you may feel are sometimes overlooked. In your answer, you should include some of the pitfalls associated with “Lift and Shift” with regard to security.

* Although the provider will manage the security of the cloud, security is the responsibility of the customer.
* Firewalls and account security are often overlooked as customer believes the provider will take care of it
* Security patches for the OS are often overlooked also as customer will install the OS and forget to apply security patches as they think the provider will update it.
* This is because the cloud provider doesn’t want to be liable for a patch destroying a system
* Some pitfalls for lift and shift is it is hard to transfer or switch to another provider

Explain what a Security Group is and what are some of the ideas that you keep in mind when designing rules. Give examples of common big picture configurations. Consider and note what you feel could be good examples of poor configuration(s).

* Never use root access as it can get compromised
* Use multiple user accounts with different permissions of only what they need to access
* Revoke credentials when people leave organizations

Explain the use of VPCs and how you utilize them. What networking technology does a VPC resemble.

* A virtual private cloud that has a virtual network
* Can define what the cloud talks to engress/ingress

What are some of the best practices for Security In the Public Cloud?

* **To patch OS running in the cloud**
* **Have 2FA on accounts that login into the cloud**
* **Manage privileges of accounts operating/interacting with the cloud**
* **To deny all traffic except what is needed**
* **To use different regions of the cloud**

Do any of the security approaches differ in the Public Cloud than they do in on premise deployments?

* It is best practice to use different locations of the cloud to maximize backups
* When on premise security a deployment wont be live for anybody if a mistake happens vs on the cloud security mistake can go live right away.

Did you find any any providers guidance (AWS, etc.) associated with security considerations?

**Systems Availability:**

What issues does Public Cloud computing solve with regard to offering higher availability for applications of delivery / content delivery and “uptime”?

Latency by providing multiple regions for the clouds location

How would you go about determining what your minimum level of infrastructure is with regard to regions and availability zones. Said differently, what is the minimum number of regions and availability zones that you should consider architecting when running / delivering a “mission critical” service / application for your organization.

* You would want your infrastructure where most of your traffic/assets are
* To make sure if one region has a disaster, the other region will most likely be safe
* And to have enough in the region to provide low latency but also be disaster safe

How are regions and availability zones utilized provide increased application resilience, availability, and performance.

* **To have multiple cloud locations in the same region to provide low latency**

**Practical:**

**Overview:**

Configure an Instance that is accessible to connections originating from the campus public gateway

**High Level Steps:**

**Useful Resources:**

**Cloud Migration**

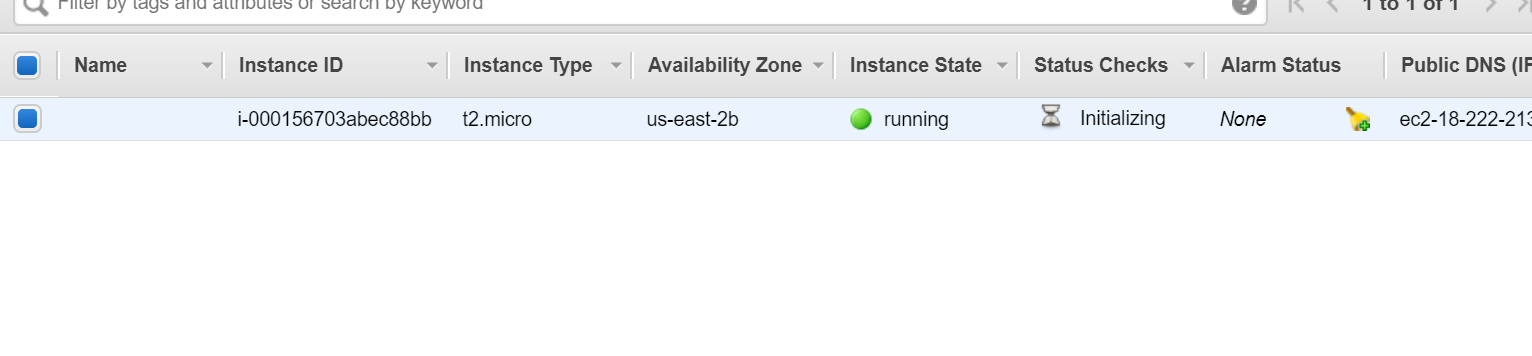
https://aws.amazon.com/blogs/publicsector/aws-cloud-migration-guide-methodology-for-migration-readiness-and-cloud-adoption/

**(Public) Cloud Security Guidance**

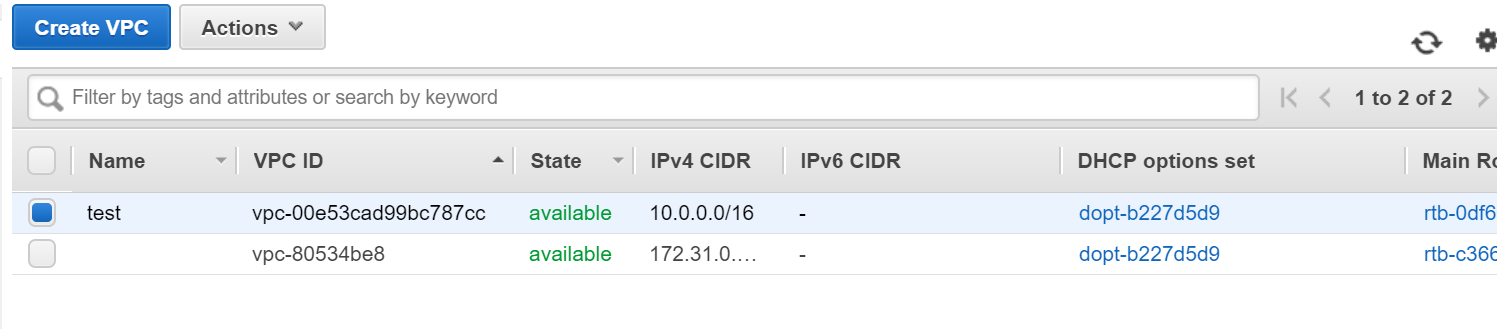
https://aws.amazon.com/blogs/security/auditing-security-checklist-for-aws-now-available/

**Documentation:**

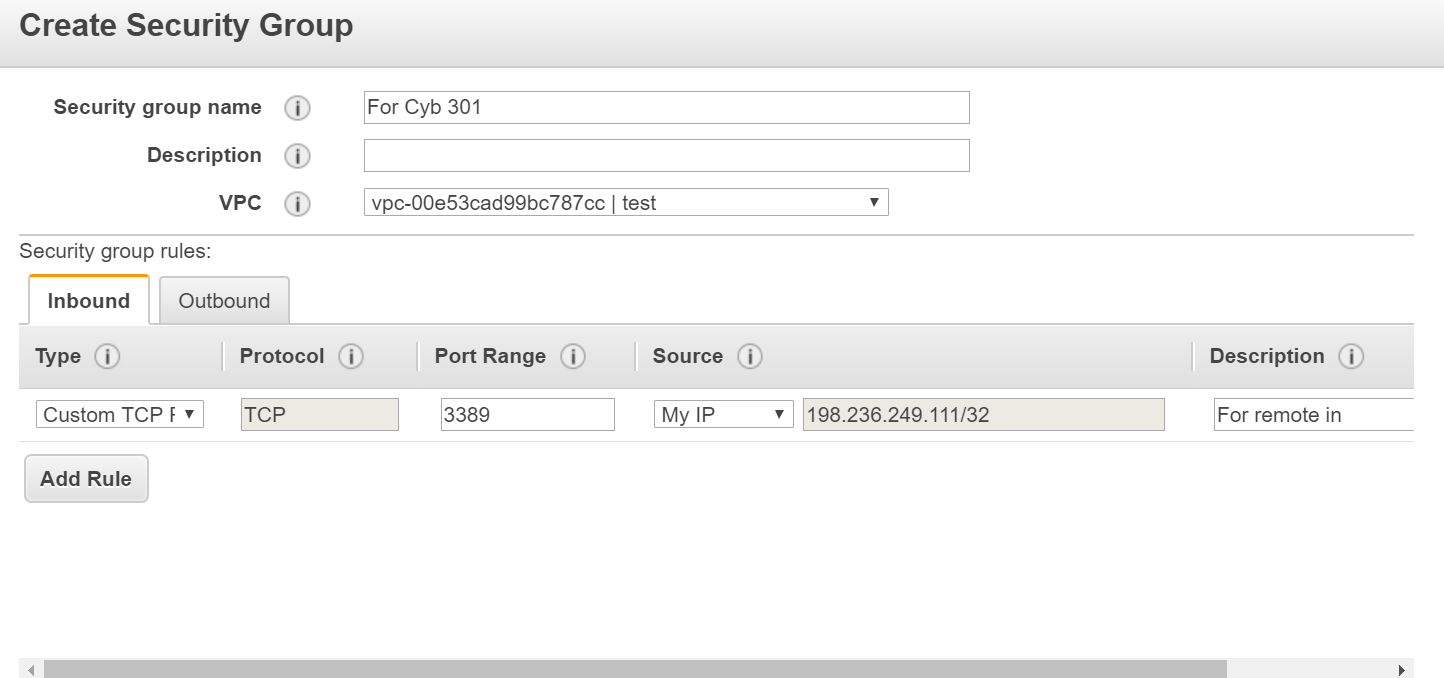
Configure an EC2 instance (of any operating system that you prefer)



Configure VPCs so that servers are adequately isolated (explain your reasoning)



Configure Security Groups for local (in AWS) and remote (from AWS to on premises office) (explain your rules)



* Only allow remote in from my ip address
* Only allow http and https traffic outbound