Security in Cloud Computing and IoT
Lab 1

1. AIM:

The aim of this experiment is to implement a cloud security policy and to analyze and mitigate security risks in IaaS, PaaS, and SaaS cloud service models using AWS Security Hub.

2. REQUIREMENTS:

Software Requirements:

- AWS Account
- AWS Config
- AWS Security Hub
- Amazon EC2
- Amazon RDS
- AWS IAM

3. INTRODUCTION

Cloud computing provides services over the internet, but security is a major concern. If cloud resources are not configured properly, they can be exposed to attackers. AWS provides Security Hub, which continuously checks the security posture of cloud resources and reports security issues called findings.

In this experiment:

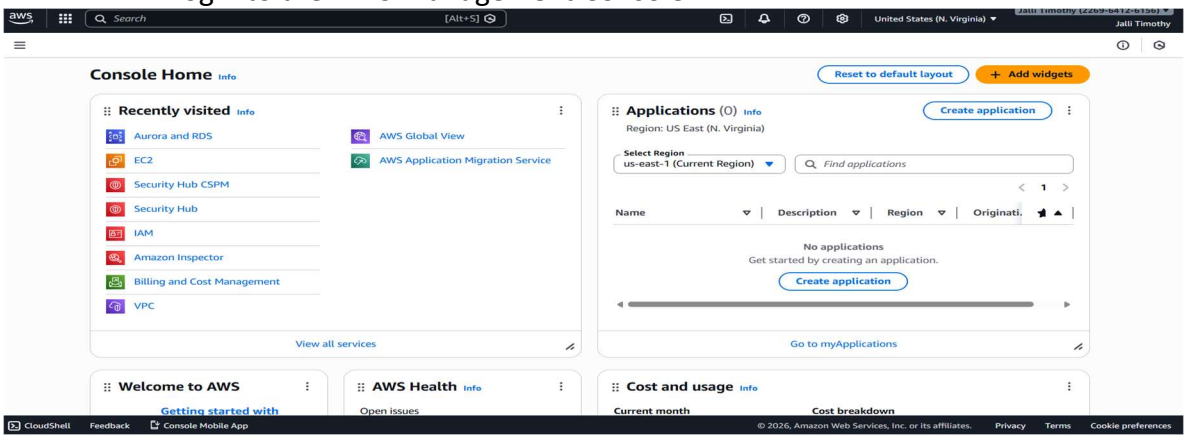
- EC2 is used for IaaS
- Amazon RDS is used for PaaS
- IAM is used for SaaS

4. PROCEDURE

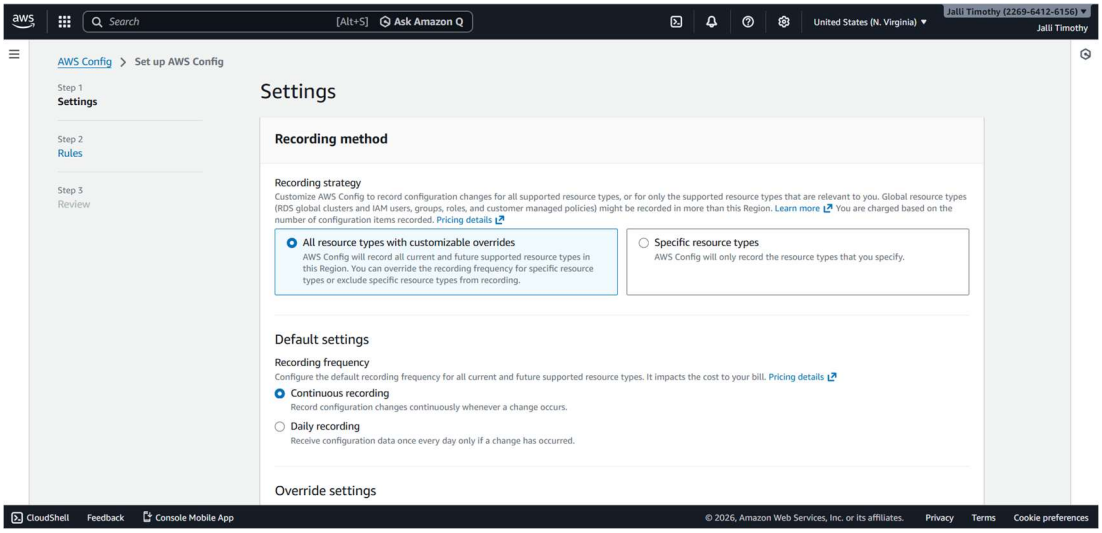
4.1. STEP1: ENABLE AWS CONFIG

AWS Config is used to record and track configuration changes of AWS resources. AWS Security Hub depends on AWS Config to evaluate security controls. Without enabling AWS Config, Security Hub findings may be inaccurate.

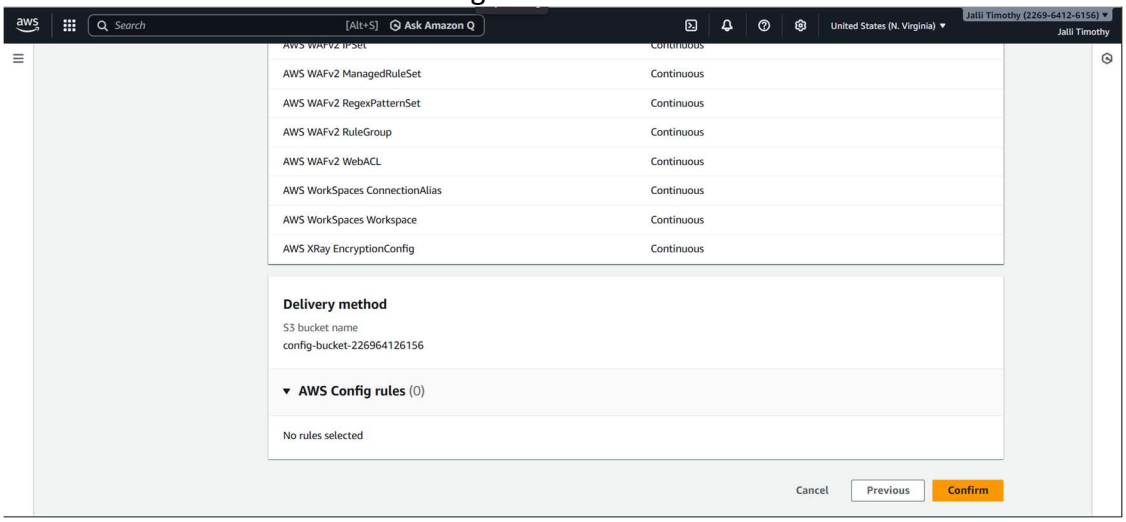
- **Steps**
  1. Login to the AWS Management Console



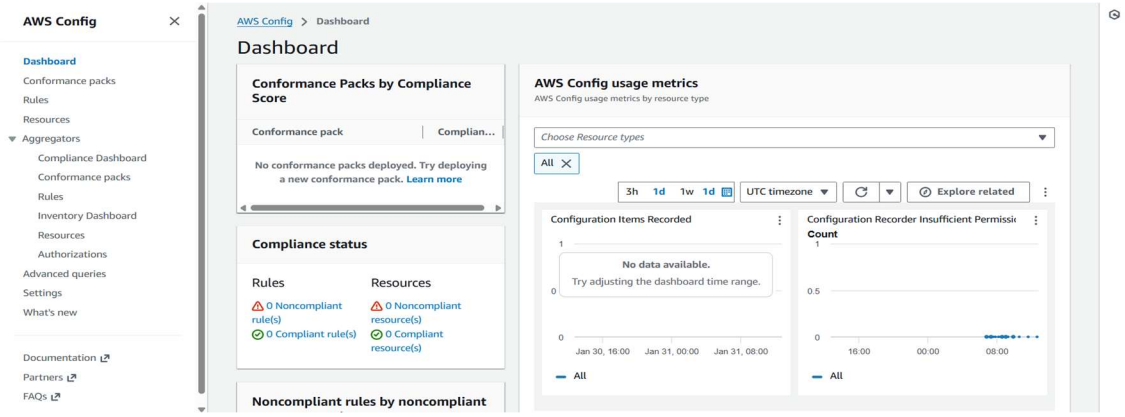
2. Search for AWS Config
3. Click Get started



4. Enable Resource recording



5. Select Record all resources
6. Choose Service-linked role
7. Click Confirm



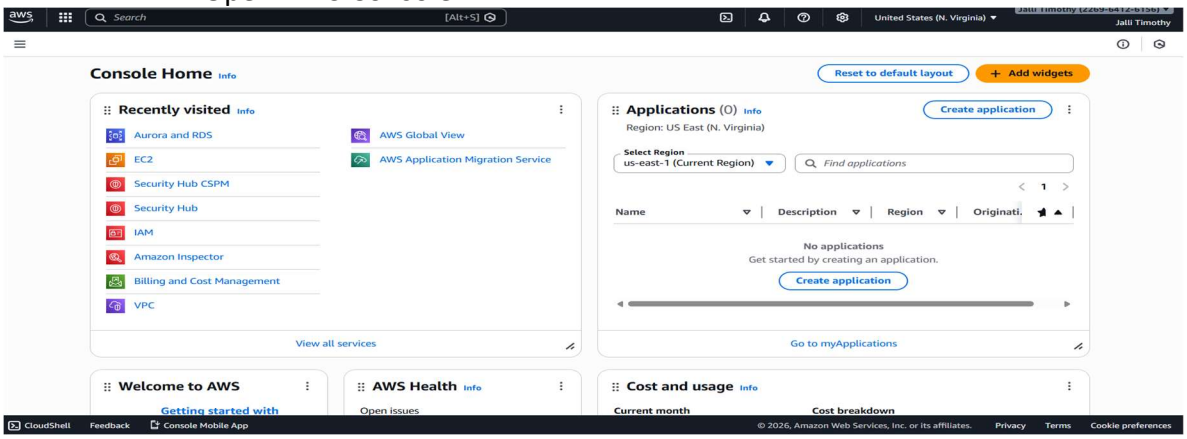
AP25122050007, AP25122050013, AP25122050027

4.2. STEP 2: ENABLE AWS SECURITY HUB

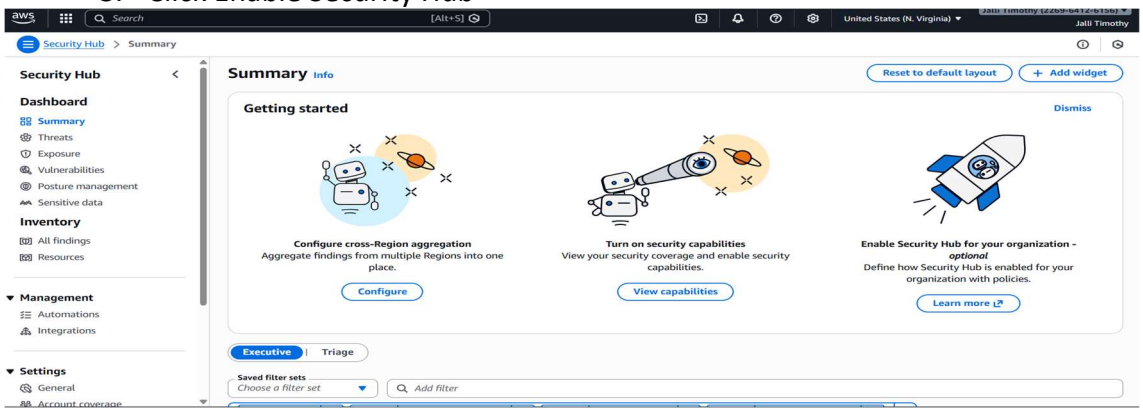
AWS Security Hub is a centralized security service that collects findings from AWS services and checks resources against security standards like CIS and AWS Foundational Security Best Practices.

- **Steps**

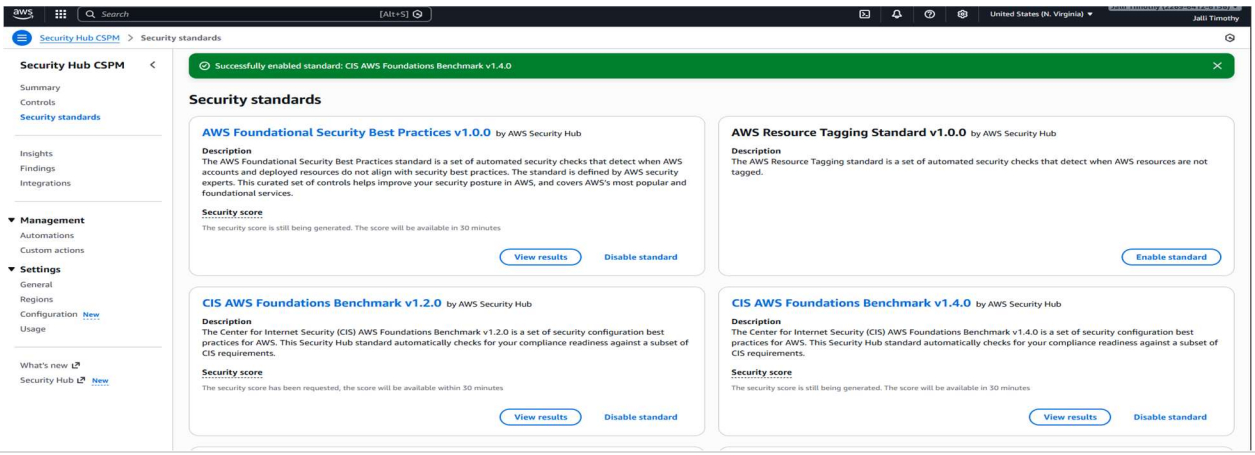
1. Open AWS Console



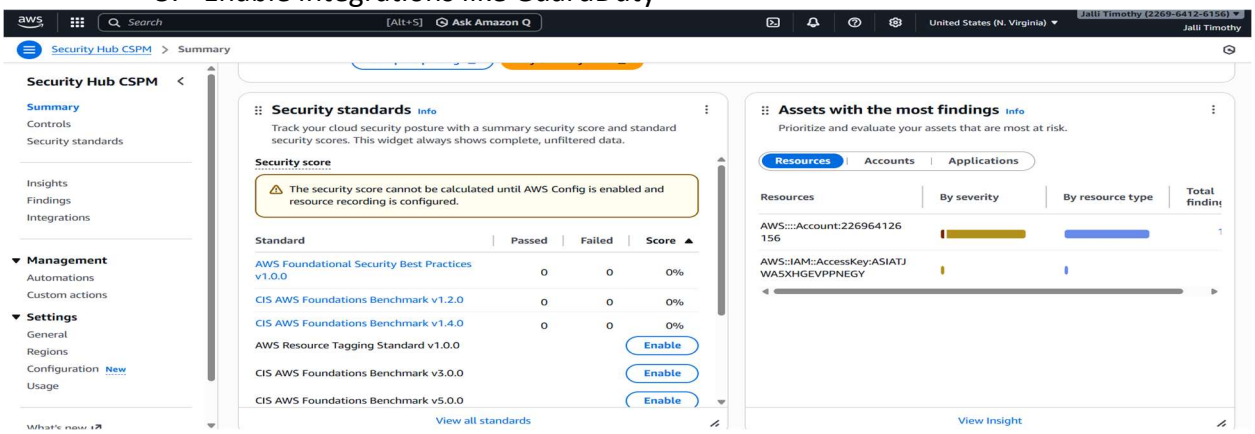
2. Search for AWS Security Hub
3. Click Enable Security Hub



4. Enable security standards:
   - AWS Foundational Security Best Practices
   - CIS AWS Foundations Benchmark



5. Enable integrations like GuardDuty

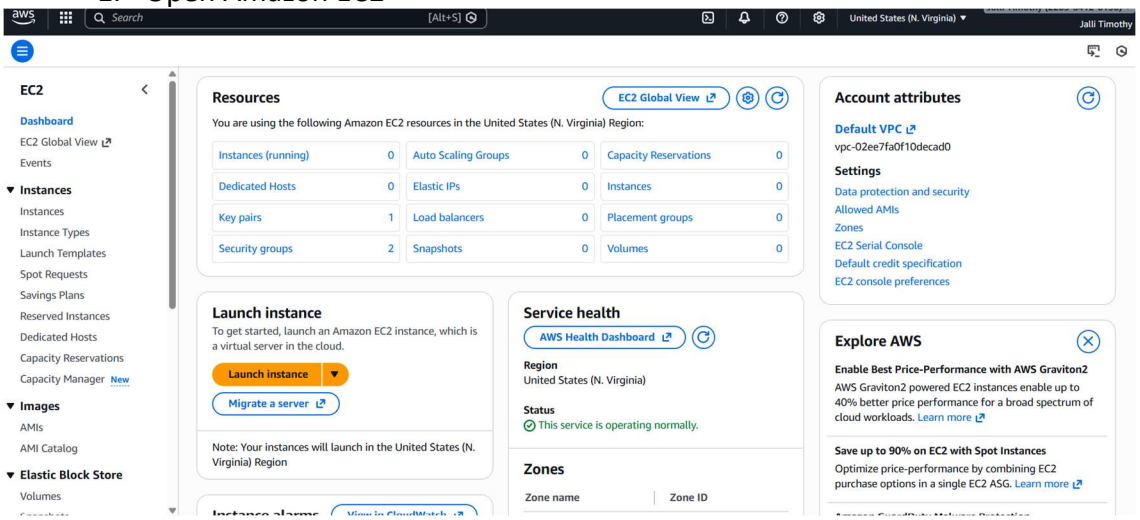


4.3. STEP 3: IaaS RISK ANALYSIS – AMAZON EC2

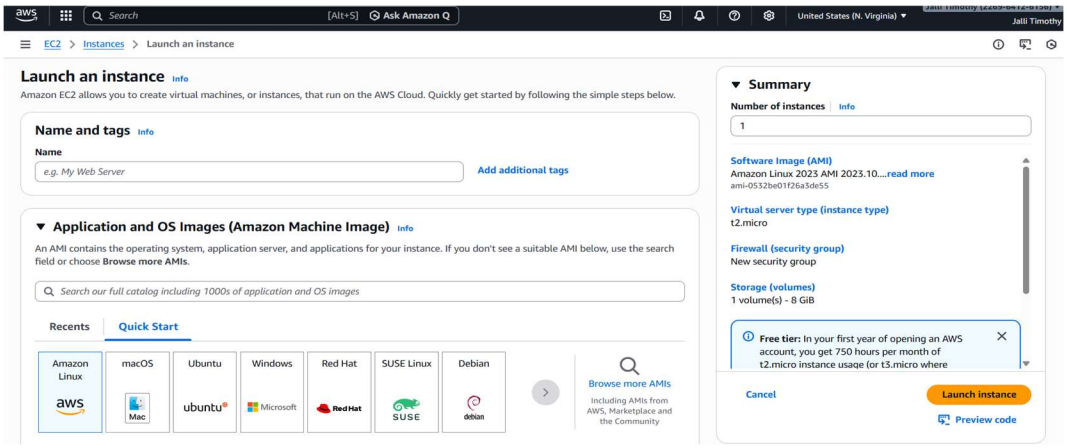
Amazon EC2 is an Infrastructure as a Service (IaaS). If security groups are misconfigured, EC2 instances can be accessed by anyone on the internet.

- **Steps**

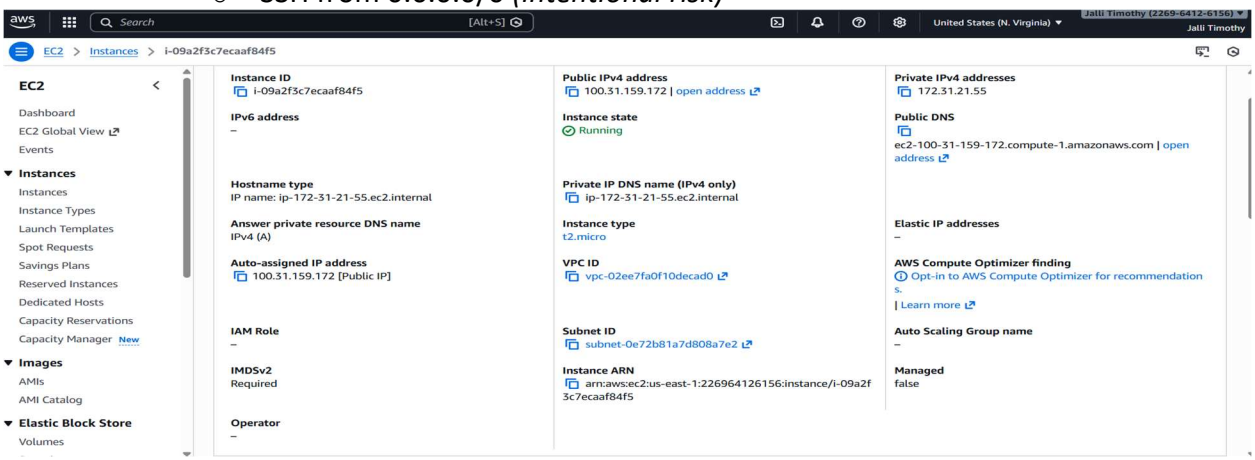
1. Open Amazon EC2



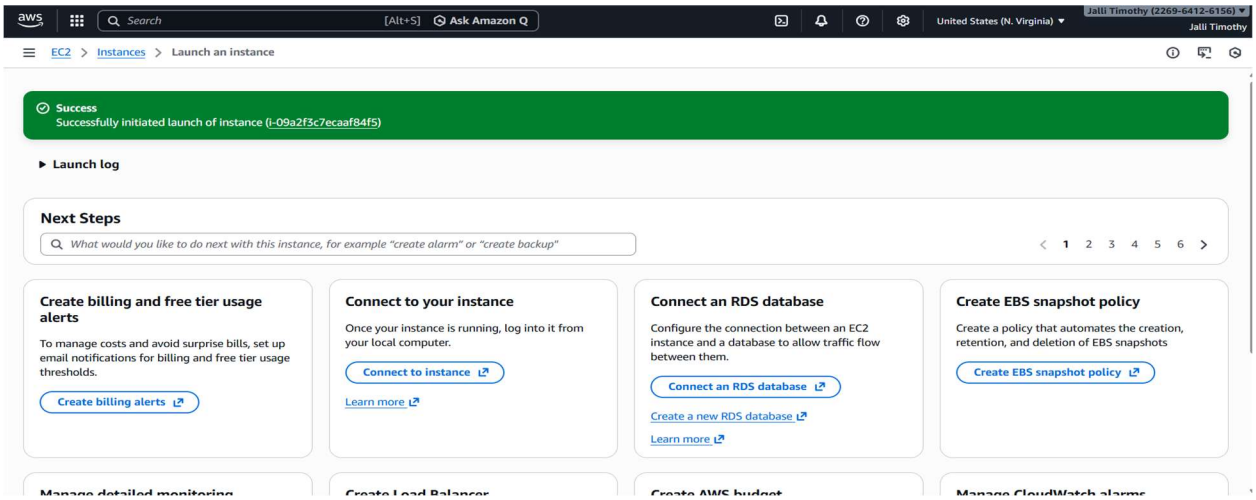
2. Click Launch Instance



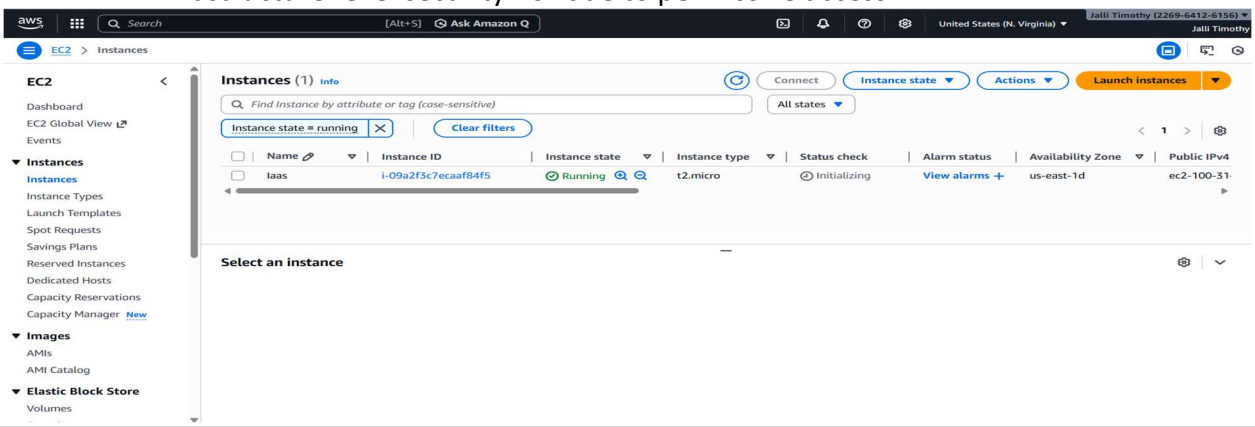
3. Choose Amazon Linux
4. Select t2.micro / t3.micro (Free Tier)
5. In Security Group, allow:
    - SSH from 0.0.0.0/0 *(intentional risk)*



6. Launch the instance

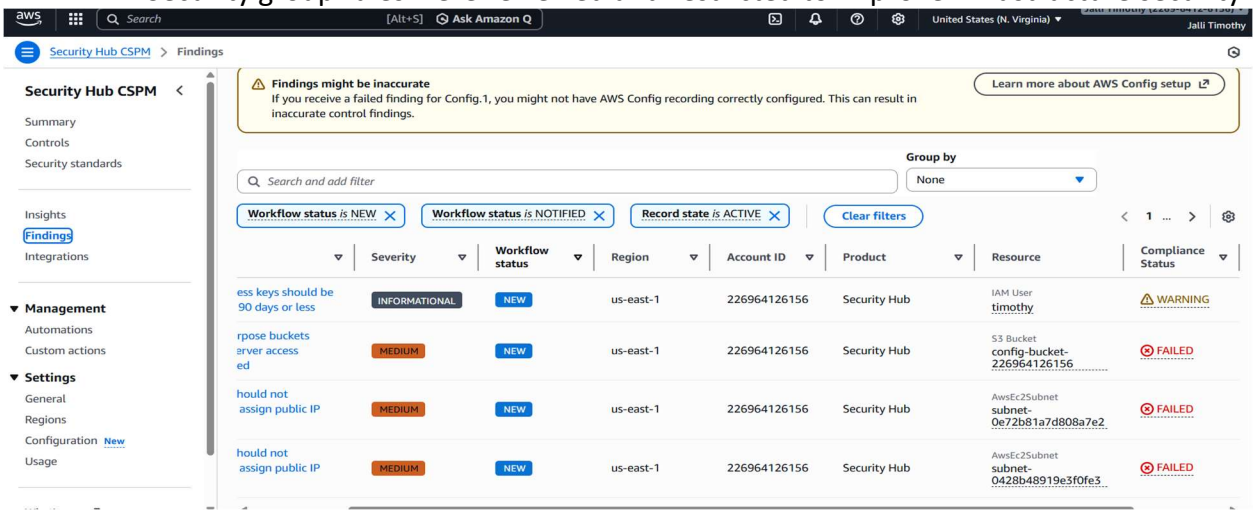


- **Finding (IaaS)**
  AWS Security Hub reported findings related to EC2 and IAM usage, indicating an infrastructure-level security risk due to permissive access.



- **Mitigation (IaaS)**

  Security group rules were reviewed and restricted to improve infrastructure security.



4.4. STEP 4: PaaS RISK ANALYSIS – AMAZON RDS

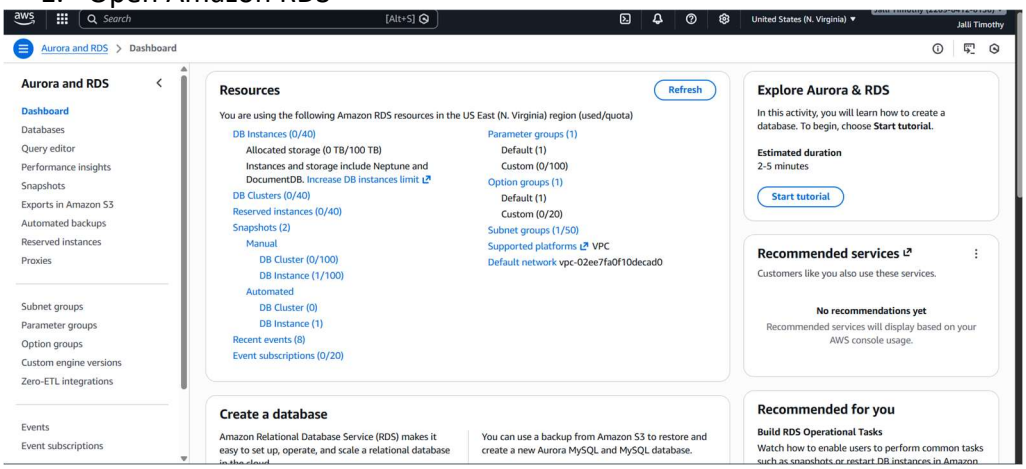
Amazon RDS is a Platform as a Service (PaaS).

A database should never be exposed to the public internet.

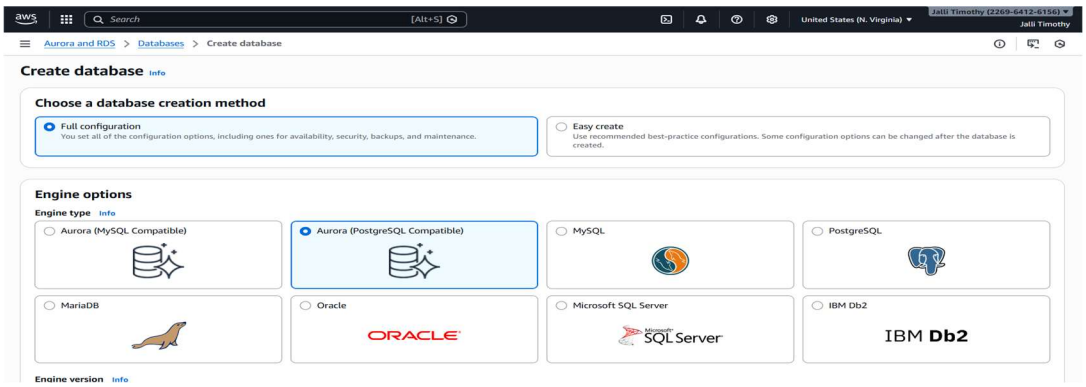
Public access to a database can lead to data breaches.

- **Steps**

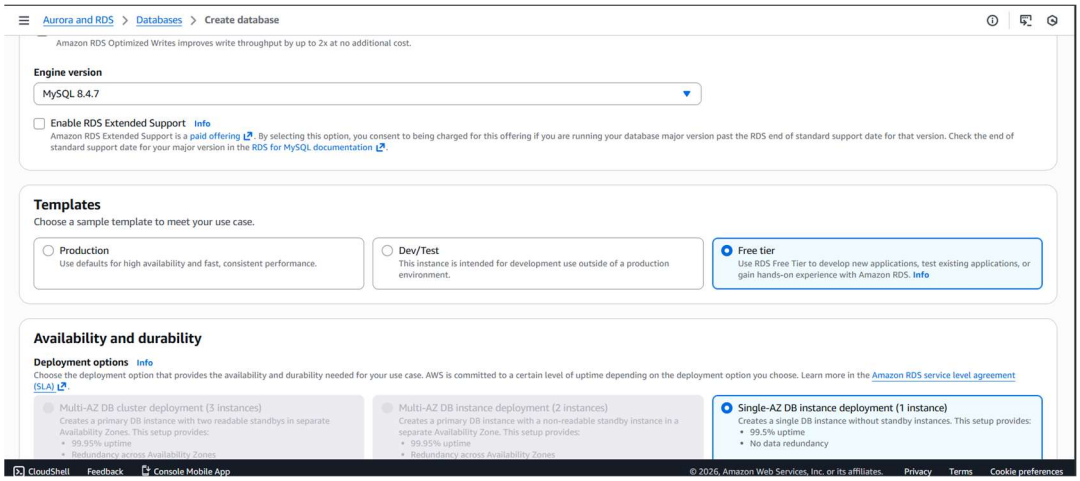
1. Open Amazon RDS



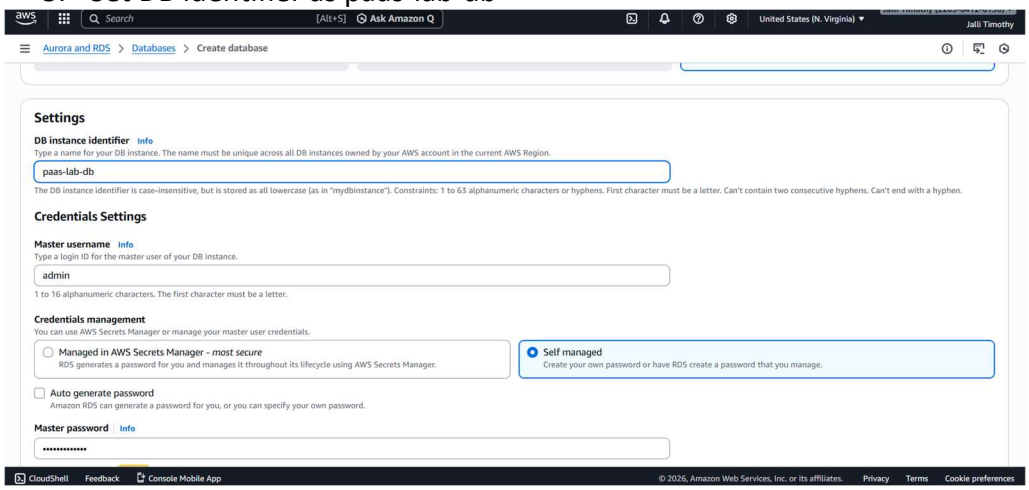
2. Click Create database



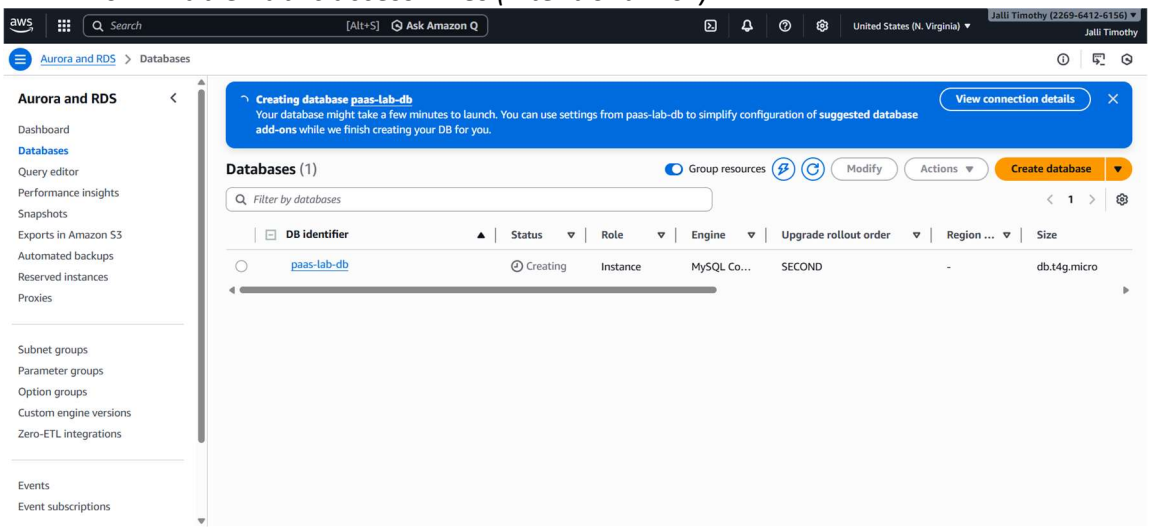
3. Select MySQL
4. Choose Free Tier



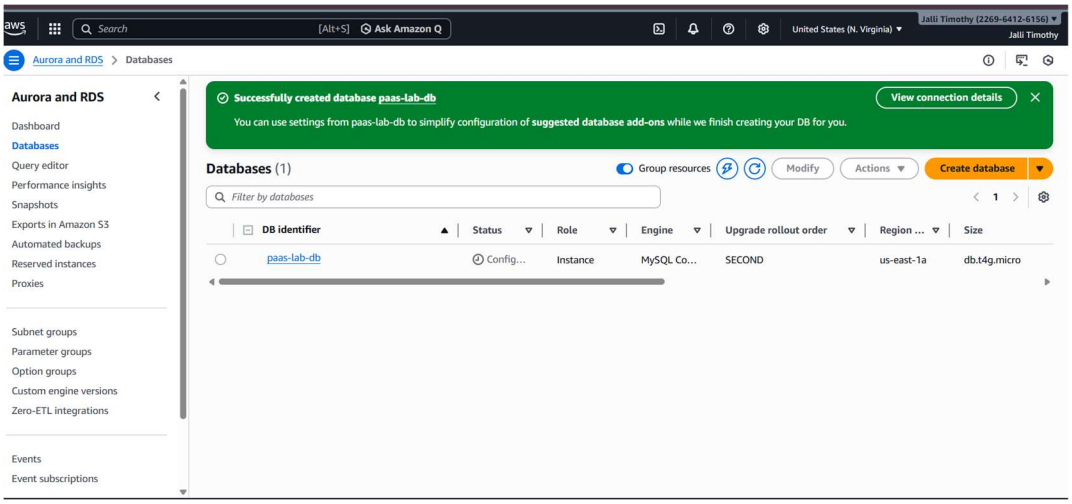
5. Set DB identifier as paas-lab-db



6. Enable Public access = Yes *(intentional risk)*

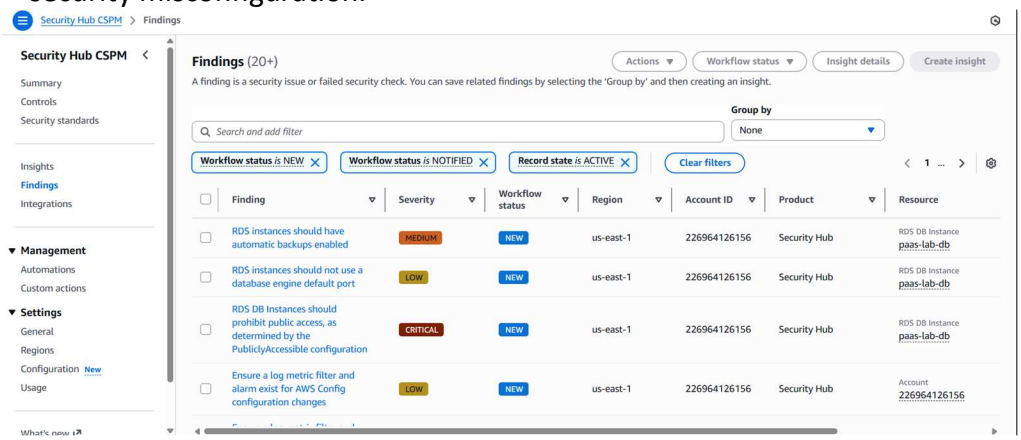


7. Create database

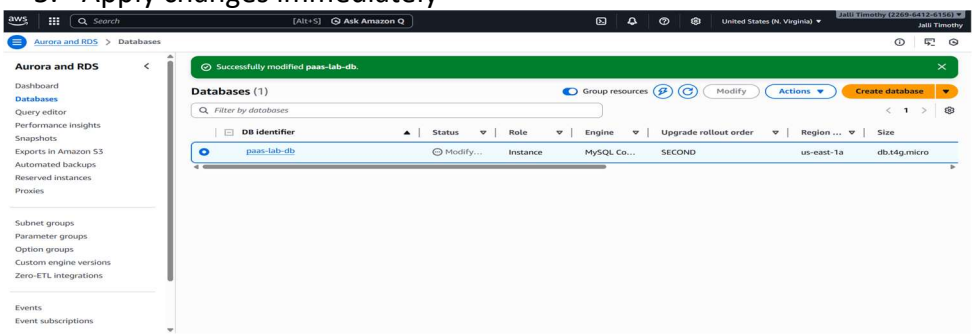


- **Finding (PaaS)**

  The RDS database was found to be publicly accessible, which represents a PaaS security misconfiguration.



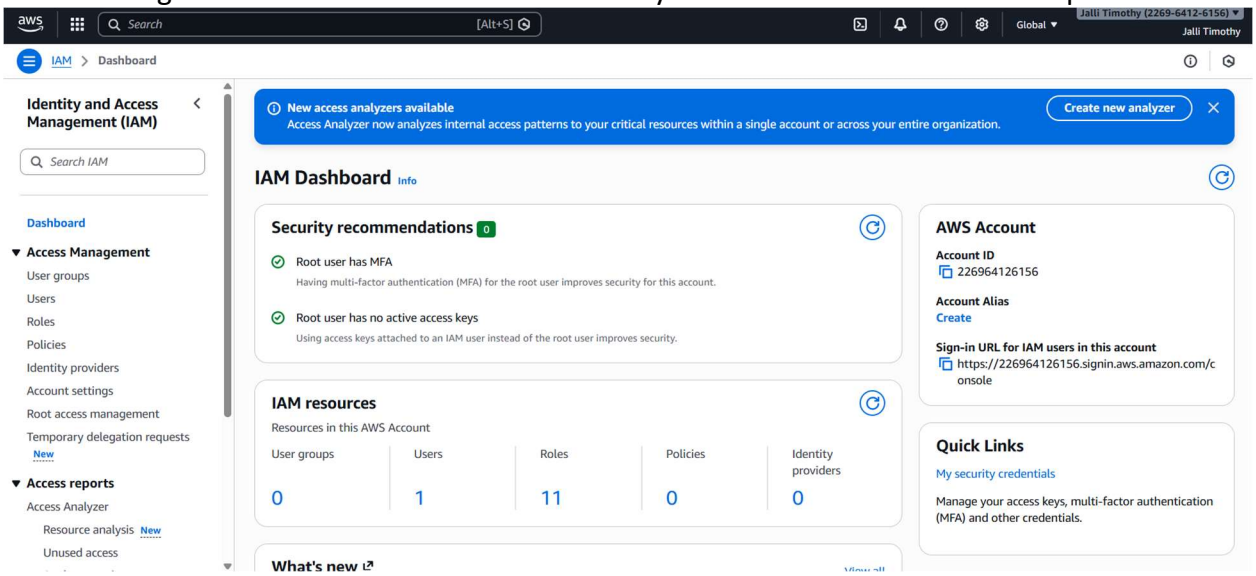
- **Mitigation (PaaS)**
  1. Go to RDS → Databases
  2. Select the database
  3. Click Modify
  4. Change Public access → Not publicly accessible
  5. Apply changes immediately



4.5. STEP 5: SaaS RISK ANALYSIS – IAM / ROOT ACCOUNT

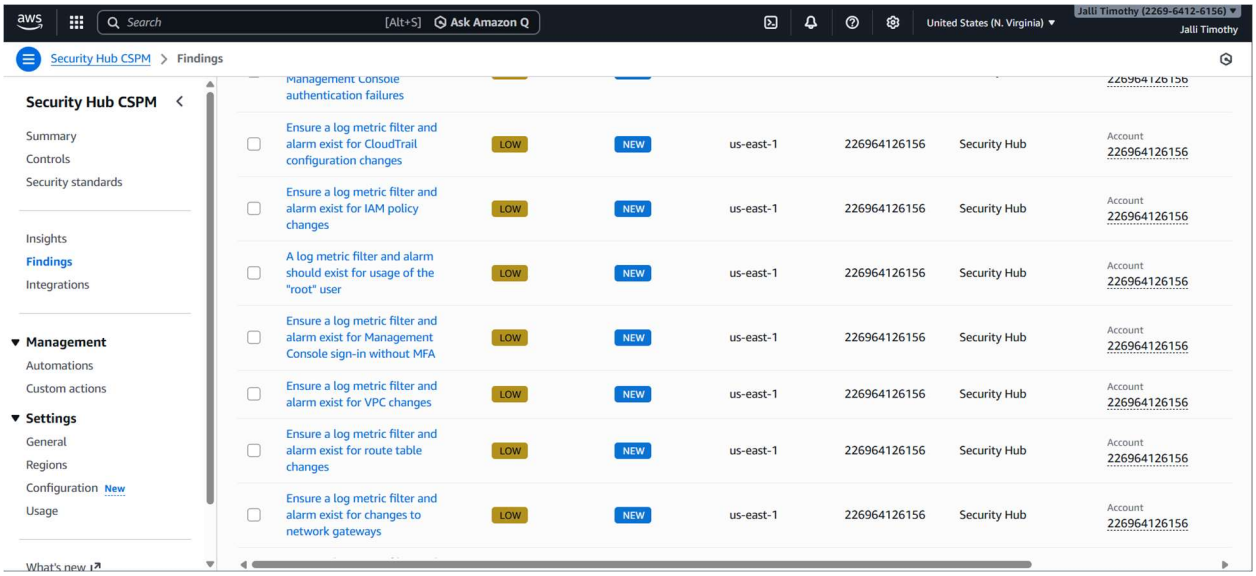
IAM is a Software as a Service (SaaS).

Using the root account without MFA is risky because the root user has full permissions.



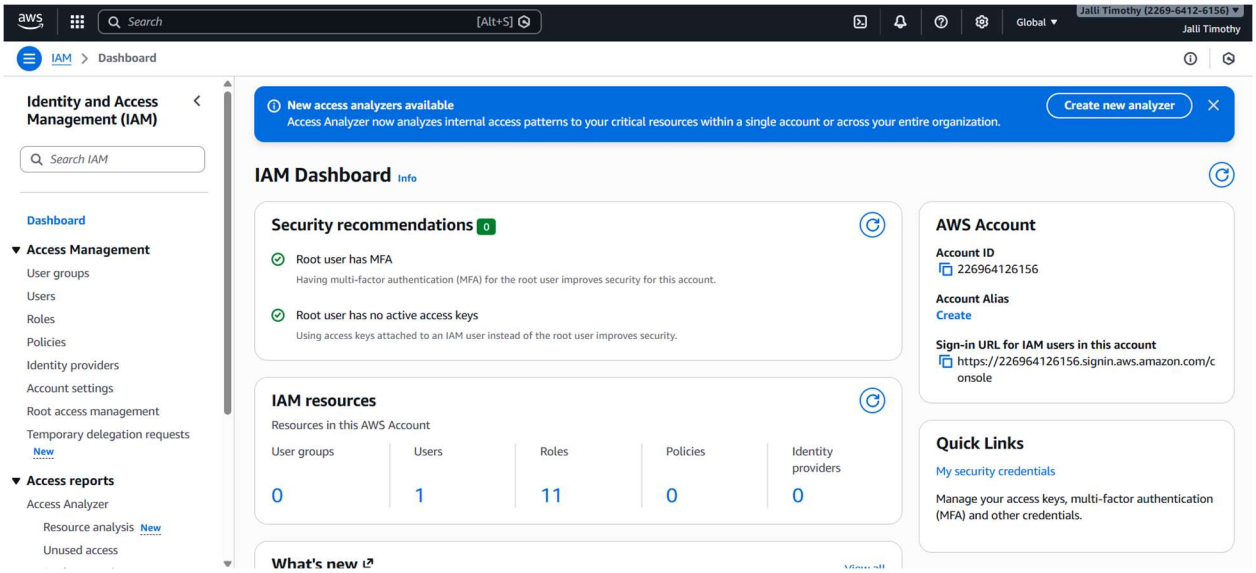
- **Finding (SaaS)**

  AWS Security Hub detected usage of root credentials, indicating a SaaS-level security issue.



- **Mitigation (SaaS)**

  1. Open IAM
  2. Go to IAM Dashboard
  3. Click Activate MFA on root account
  4. Configure Virtual MFA
  5. Complete MFA setup



5. RESULT:

All identified security risks in IaaS, PaaS, and SaaS were successfully mitigated using AWS Security Hub and AWS security best practices.

6. CONCLUSION:

This experiment helped in understanding how cloud security risks occur due to misconfiguration.

Using AWS Security Hub, security risks were identified and mitigated, thereby improving the overall cloud security posture.