National College of Ireland

Zero Trust Architecture In Cloud Environments

MSc Research Project
MSc Cybersecurity

Sivaram pakalapati
Student ID:23231131

School of Computing
National College of Ireland

Supervisor: Liam Mccabe

National College of Ireland

MSc Project Submission Sheet

School of Computing

StudentName:	Sivaram pakalapati
Student ID:	23231131
Programme:	MSc Cybersecurity **Year:** 2024
Module:	Practicum Part2
Lecturer:	Liam Mccabe
Submission Due Date:	12/12/2024
Project Title:	Zero Trust Architecture in Cloud environments
Word Count:	959 **Page Count:** 10

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: ……p.sivaram……

Date: ……12/12/2024……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Sivaram pakalapati
Student ID: 23231131

1 Introduction

This document provides a comprehensive guide to the configuration and setup of the AWS environment for the MSc research project titled Zero Trust Architecture in Cloud Environments. The project aims to implement a robust cloud infrastructure based on the Zero Trust security model, ensuring that no entity, whether internal or external, is inherently trusted.
The primary objective of this configuration is to establish a secure, scalable, and resilient environment utilizing key AWS components, including:

- Identity and Access Management (IAM)- To enforce strict user permissions and implement multi-factor authentication (MFA), following the principles of Zero Trust to verify each access attempt.
- Elastic Compute Cloud (EC2)- For scalable compute resources, configured with hardened instances and secure access controls to minimize attack surfaces.
- Virtual Private Cloud (VPC)- To create isolated network segments, enforce traffic inspection, and implement micro-segmentation, a core aspect of Zero Trust Architecture.

The setup prioritizes granular access control, network isolation, and continuous monitoring to align with the Zero Trust framework. This manual serves as a detailed reference for the configuration process, helping maintain a secure environment throughout the project lifecycle and beyond.

2 Tools and Technologies Used

Cloud Platform - Amazon Web Services (AWS)
AWS Services

- *IAM* - Identity and Access Management
- *VPC* - Virtual Private Cloud
- *EC2* - Elastic Compute Cloud
- *CloudTrail* - Monitoring and logging
- *AWS Config* - Resource compliance
- *SSM* - AWS Systems Manager

Operating System - Amazon Linux, Ubuntu

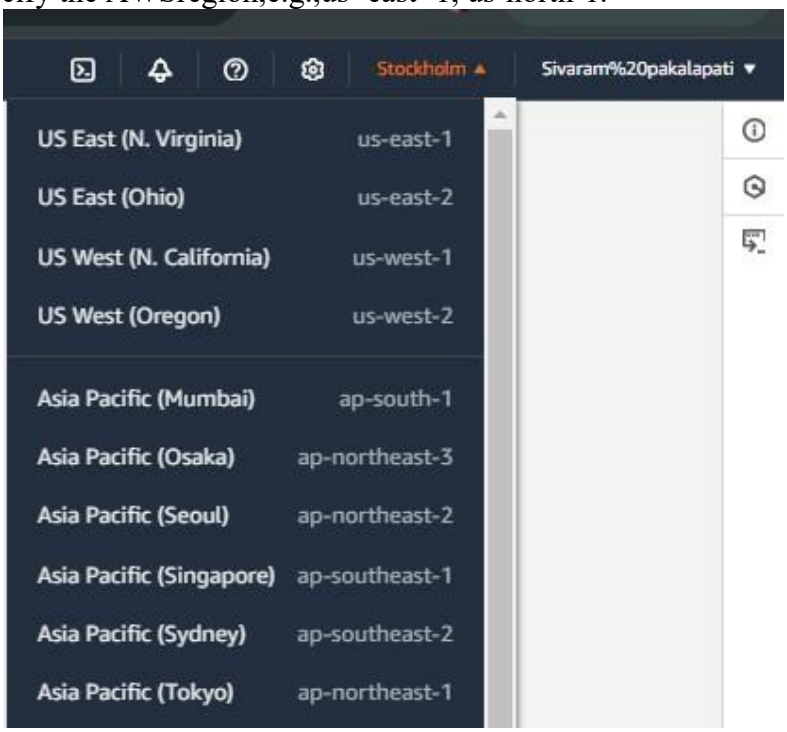
3 Project Environment

The AWS project environment was designed with a focus on security, scalability, and ease of management. The configuration includes:

- **AWS IAM for access control**: Implemented granular permissions to adhere to the principle of least privilege.
- **Amazon EC2 for compute resources**: Instances were selected based on project requirements to optimize performance and cost.
- **VPC for network isolation**: Configured with subnets and routing to enhance security and control traffic flow.

Key elements of the project environment include:

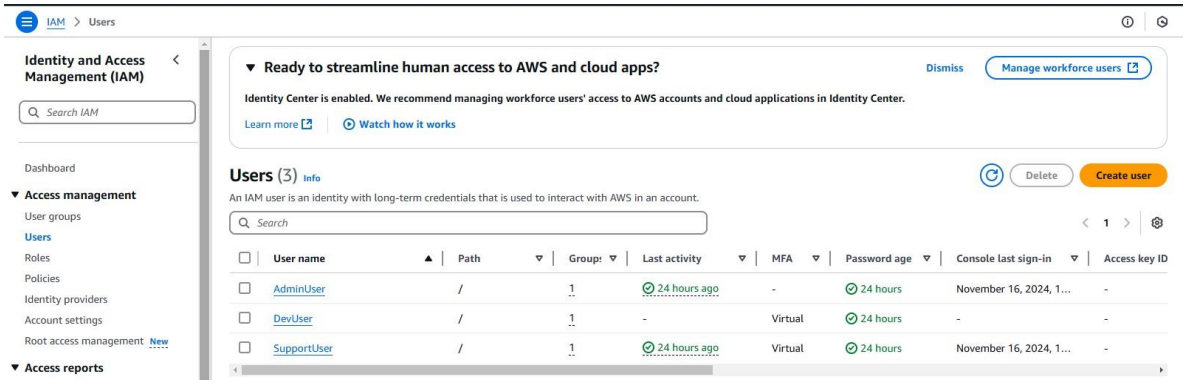
- **Region**: Specify the AWSregion,e.g.,us−east−1, us-north-1.



4 IAM Configuration

4.1.1 User Groups Setup

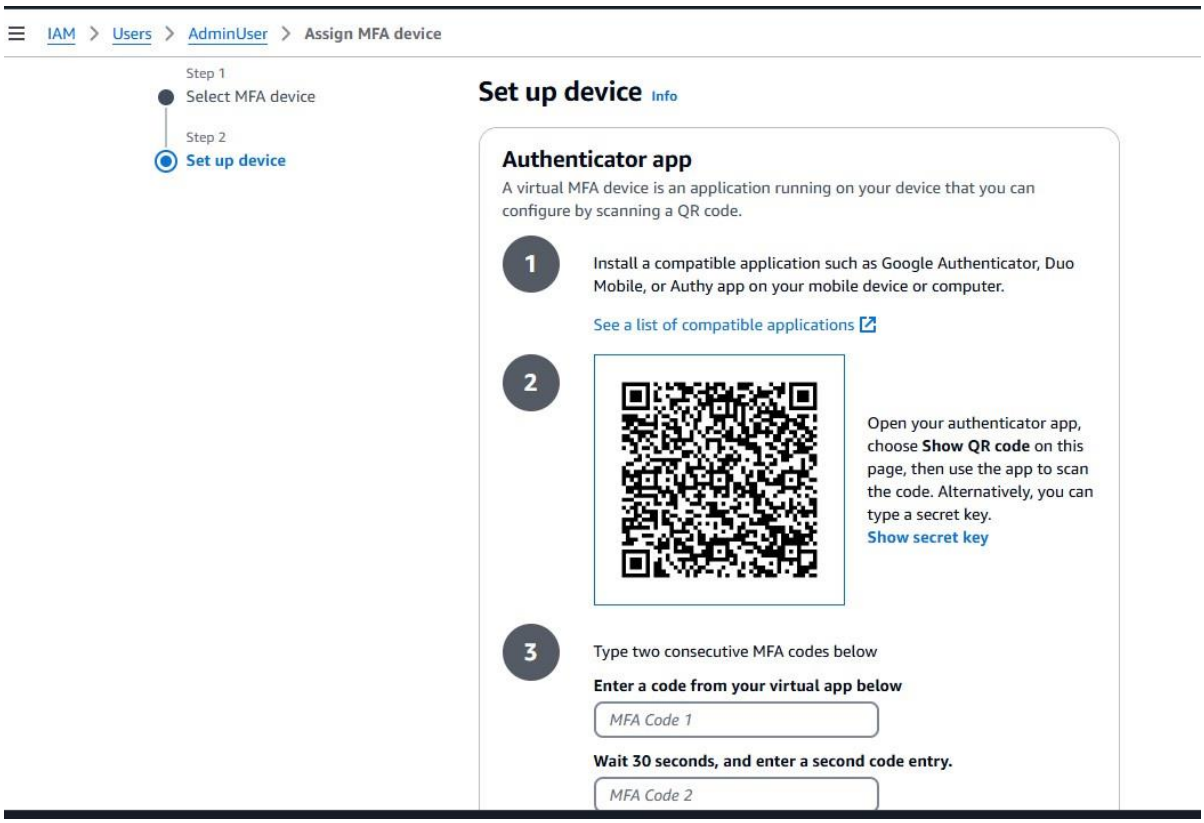
Three user groups were created to streamline access control:



1. **AdminGroup**
    - Purpose - Full access for administrative tasks.
    - Policies Attached - AdministratorAccess
    - MFA Requirement - Enabled for enhanced security.
2. **DevGroup**
    - Purpose - Developer access with limited permissions for EC2 and S3 services.
    - Policies Attached - AmazonEC2FullAccess, AmazonS3FullAccess
    - MFA Requirement - Enabled (Virtual MFA setup required for users).
3. **SupportGroup**
    - Purpose - Read-only access for monitoring and support personnel.
    - Policies Attached - ReadOnlyAccess
    - MFA Requirement - Enabled for all users to prevent unauthorized access.

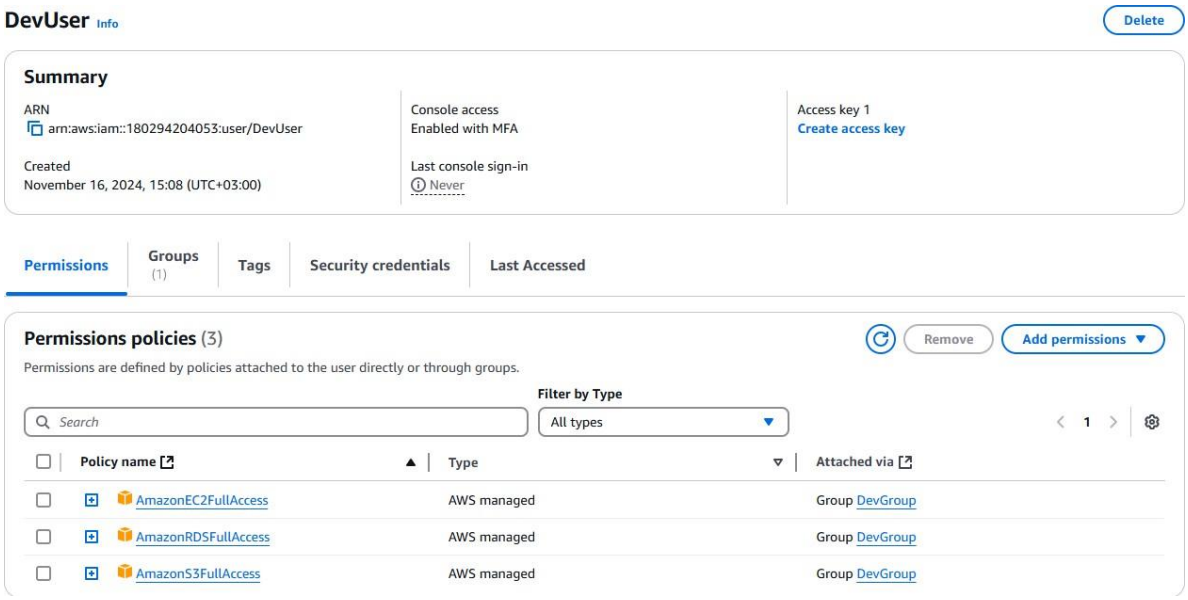
4.1.2 Enable MFA:

- Configure virtual MFA for each user using Google Authenticator or Authy.



4.1.3 Assign Roles and Policies:

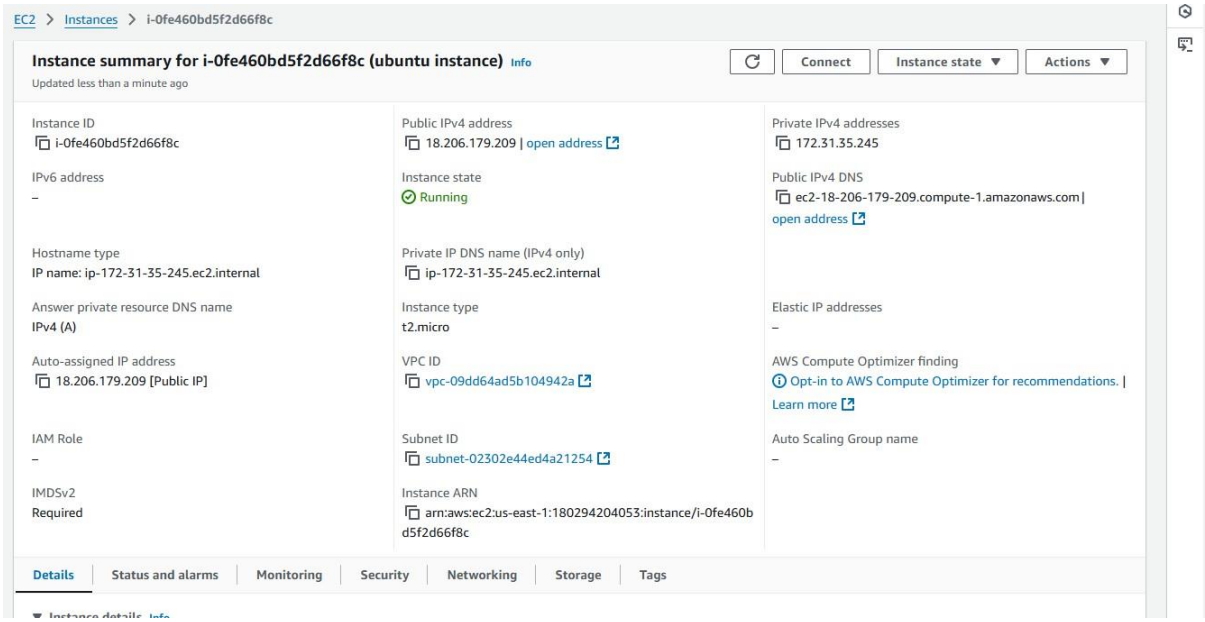
- AdminUser - Full administrative access (AdministratorAccess policy).
- DevUser - Access to EC2, S3, and Lambda (custom role with least privilege).
- SupportUser - Read-only access for troubleshooting (custom role).



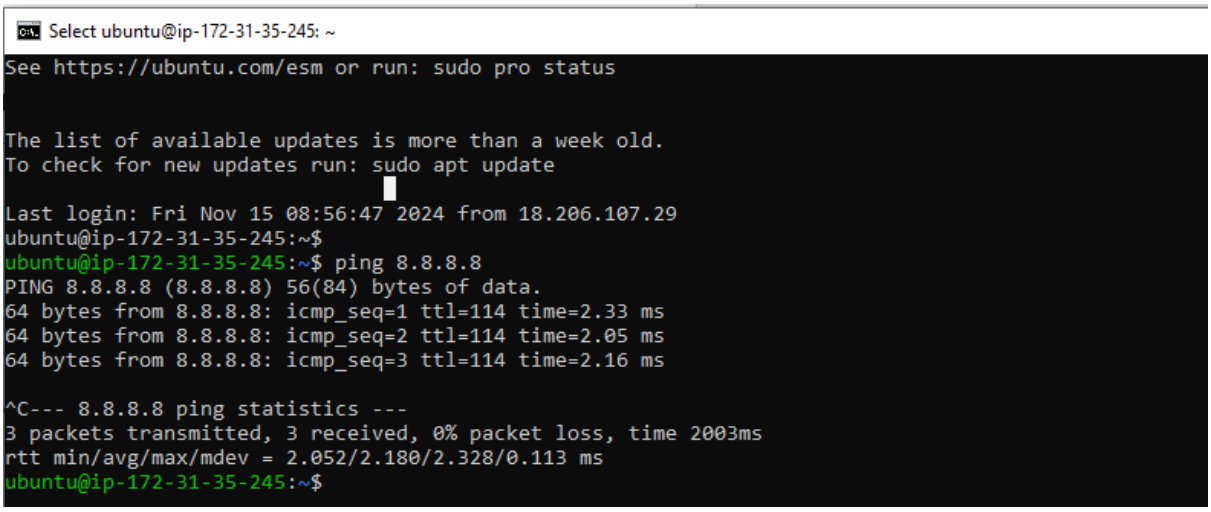
5 EC2 Configuration

5.1.1 EC2 Instances

- *Instance Type* - t2.micro for development and testing (Free Tier eligible).
- *Operating System* - Amazon Ubuntu Instance for its stability and integration with AWS services.
- *Key Pair* - Created a key pair named ProjectKeyPair for secure SSH access to instances.

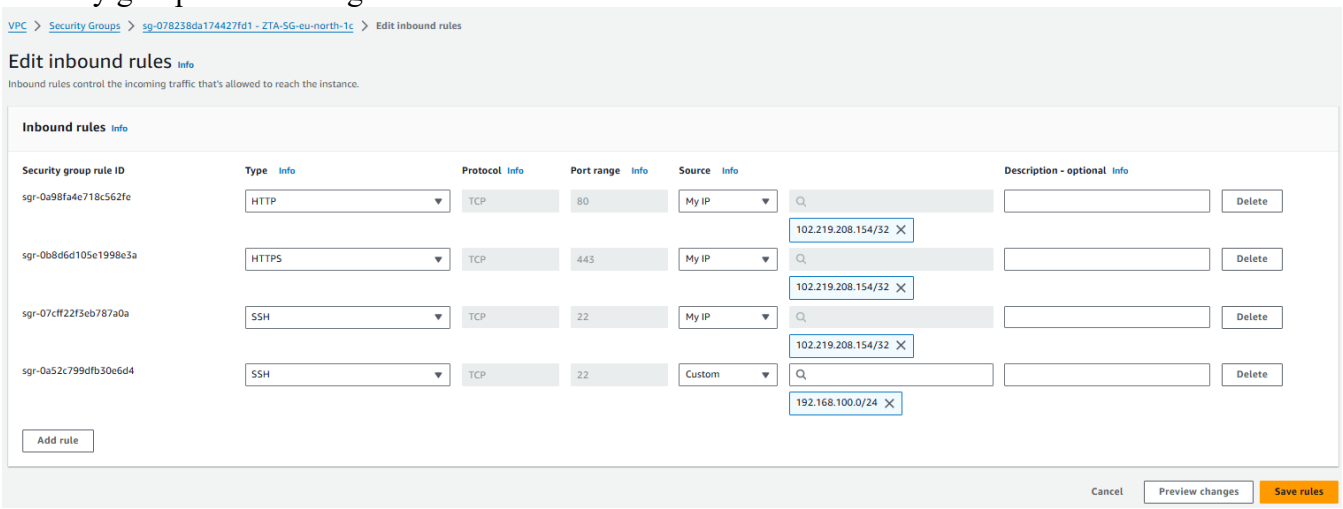


Running on ssh, you will need to give necessary permissions to the pem file, then contact administrator for add you IP address for access.



5.1.2 Security Groups

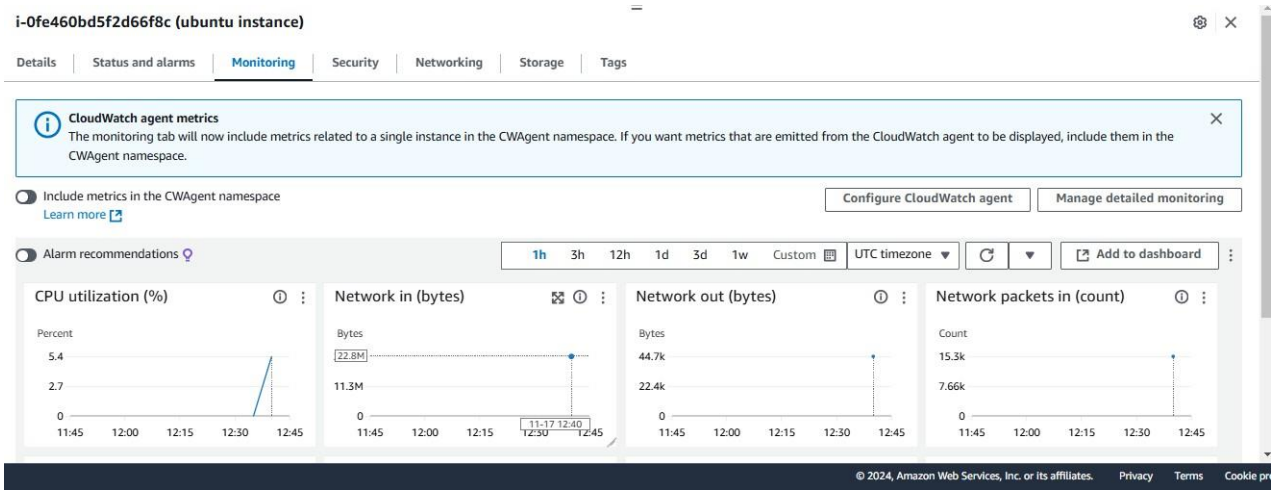
Security groups were configured as follows:



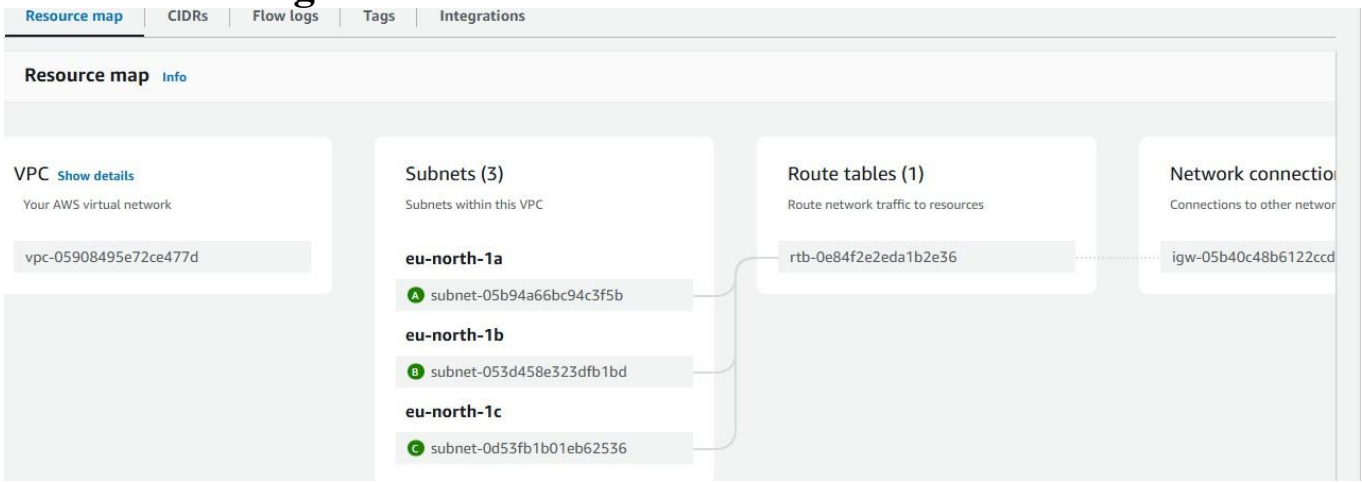
- **AdminSG**:
  - Allows unrestricted inbound traffic on all ports for administrative access (restricted by IP).
  - Outbound traffic is unrestricted for management tasks.
- **WebAppSG**:
  - *Inbound*: HTTP (port 80), HTTPS (port 443) allowed from admin IP.
  - *Outbound*: All traffic allowed.
- **SSH**:
  - *Inbound* - SSH (port 22) traffic allowed only from IP addresses allowed.
  - *Outbound*: All traffic allowed

5.1.3 Instance Monitoring and Logging

- Enabled CloudWatch monitoring for all instances.
- Configured AWS Systems Manager for centralized management and automation.

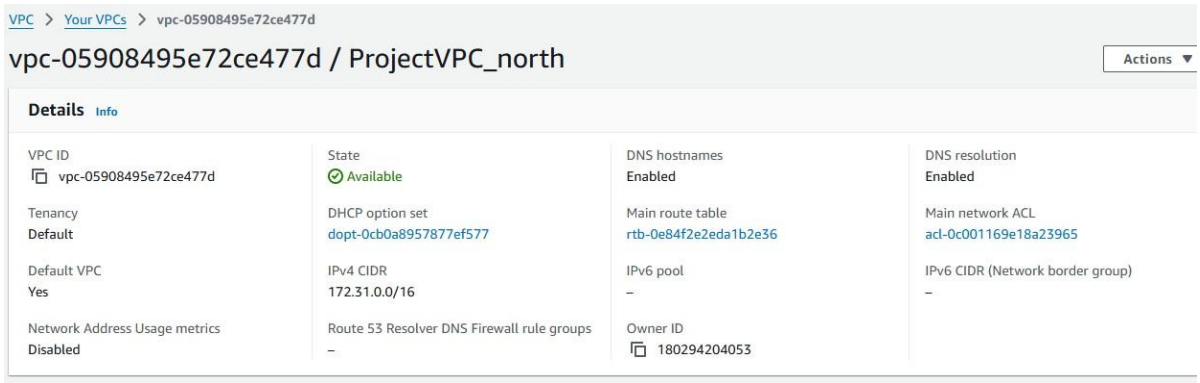


6 VPC Configuration

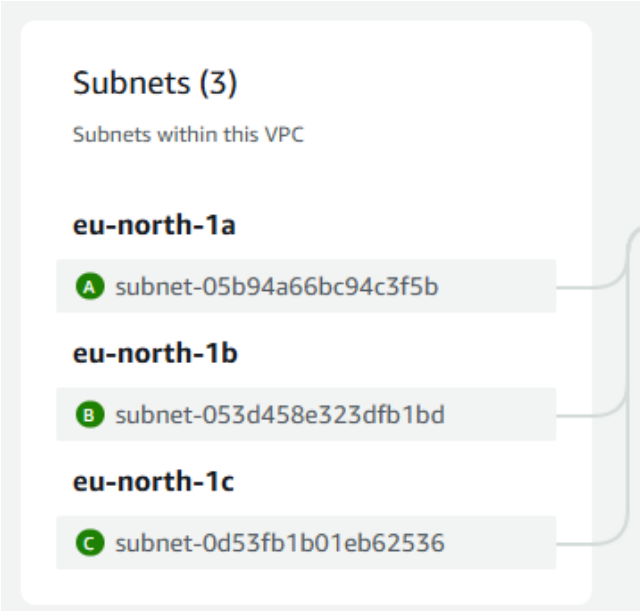


6.1.1 VPC and Subnet Design

- *VPC Name* - ProjectVPC_north
- *CIDR Block* - 172.31.0.0/16

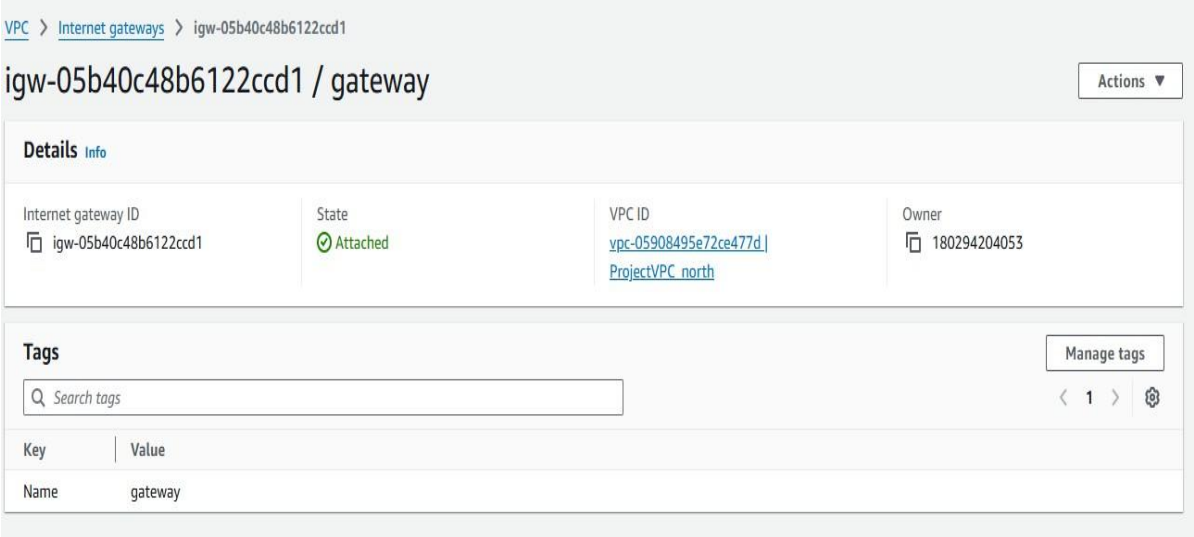


- **Subnets**:



6.1.2 Internet Gateway and NAT Gateway

- An Internet Gateway was attached to enable internet access for resources in the public subnet. A NAT Gateway was created to allow instances in the private subnet to access the internet securely.



6.1.3 Route Tables

- Configured a main route table for public subnet traffic via the Internet Gateway.
- A separate route table was created for the private subnet to route internet-bound traffic through the NAT Gateway.