CHAPTER 4
IMPLEMENTATION AND FINAL RESULTS OF CREATING VIRTUAL DATA CENTER USING AWS AND DATADOG

4.1. Preface

This chapter details the implementation process and final results of creating a Virtual Data Center (VDC) using AWS and Datadog. It includes a step-by-step explanation of the setup, configuration, and integration of various AWS services and Datadog for monitoring and analytics. The VDC was designed to be both scalable and flexible, allowing for future expansions and integrations with additional cloud services. The VDC was engineered to accommodate evolving organizational needs with minimal disruption. The final section presents the outcomes, demonstrating the efficiency and effectiveness of the implemented VDC in managing and monitoring IT infrastructure. The steps are as follows:

- Step-By-Step Guide to Create and Sign Up an AWS Root Account
- Assign Mati-Factor Authentication (MFA) for Root User and Create Alias
- Create IAM User, Assign MFA for IAM User and Sign Up
- Sequential Guide to Configure S3 (Simple Storage Service)
- Detailed Instructions for Deploying DynamoDB
- Create Role for EC2 to Access S3 and DynamoDB
- Step-By-Step Guide to Create Virtual Private Network (VPC) and Set Up Network Configuration
- Step-By-Step Guide to Launch Elastic Compute Cloud (EC2)
- Sign Up Datadog Monitoring Framework
- Integrate Datadog with AWS
- Testing and Validation

4.2. Step-By-Step to Create and Sign Up an AWS Root User Account

Visit “aws.amazon.com” to create an AWS account as shown in Figure 4.1.

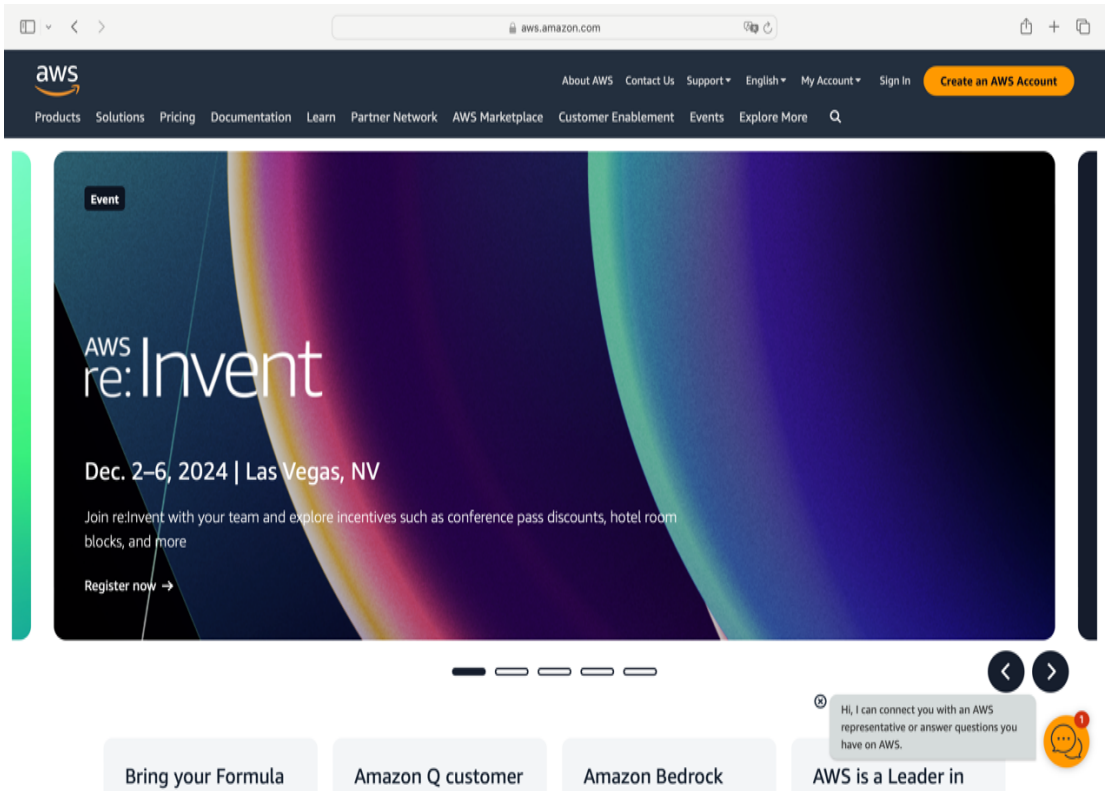


Figure 4.1. Creating AWS Account

Enter account information – Unique Email address and AWS account name as presented in Figure 4.2.

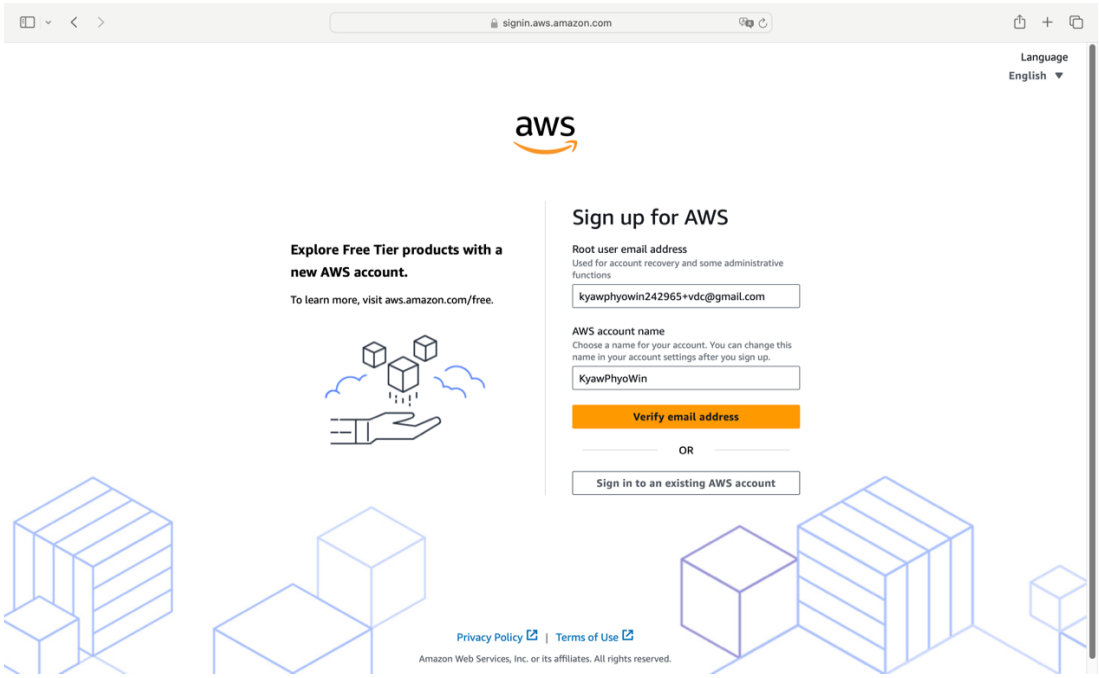


Figure 4.2. Creating AWS Account

Figure 4.3.displayed enter verification code that sent to email from AWS.

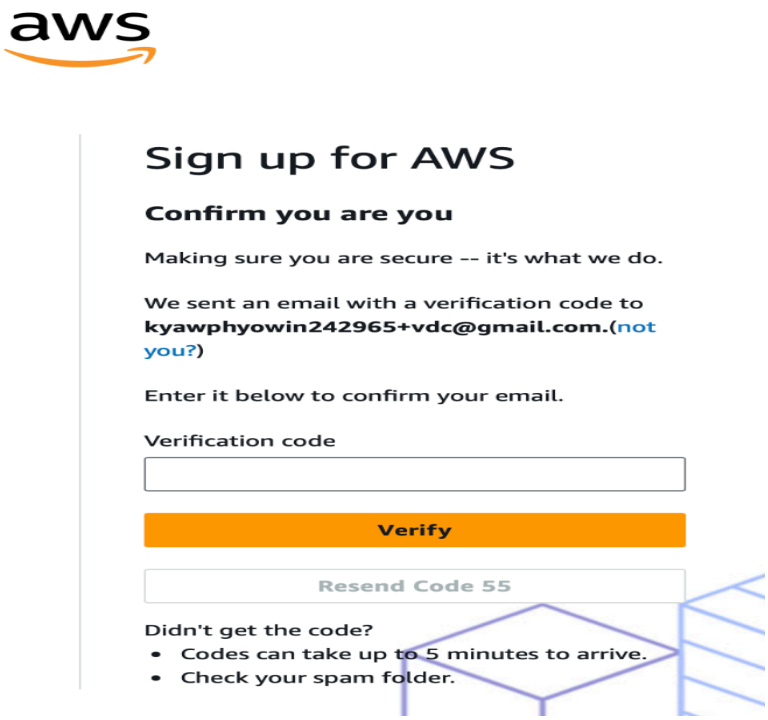


Figure 4.3. Creating AWS Account

As shown in Figure 4.4 fill and confirm password for root user.

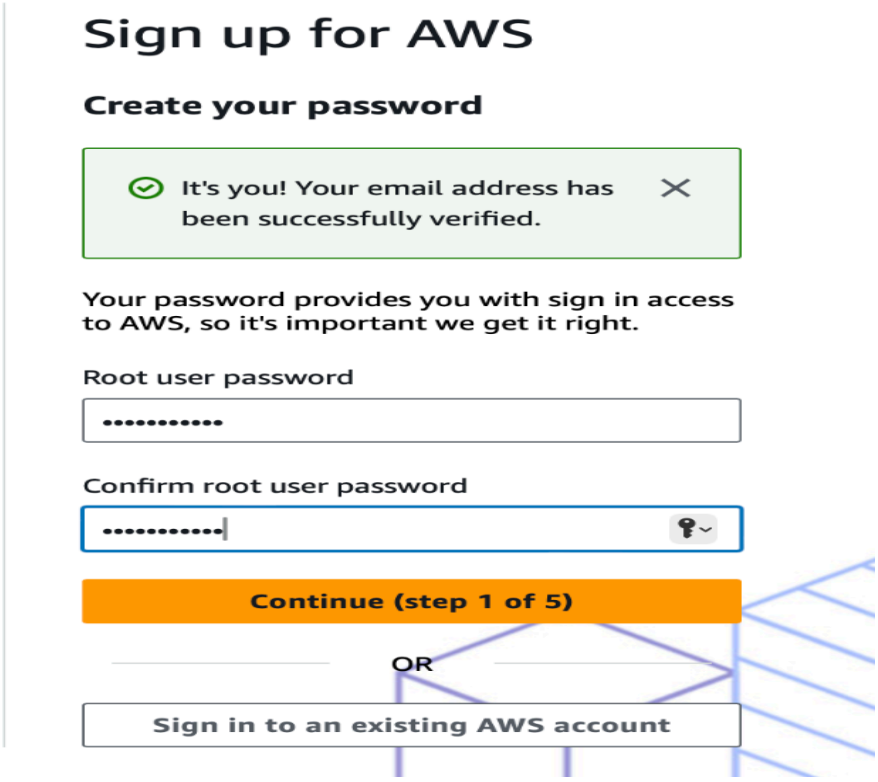


Figure 4.4. Creating AWS Account

Enter payment information as demonstrated in Figure 4.5.

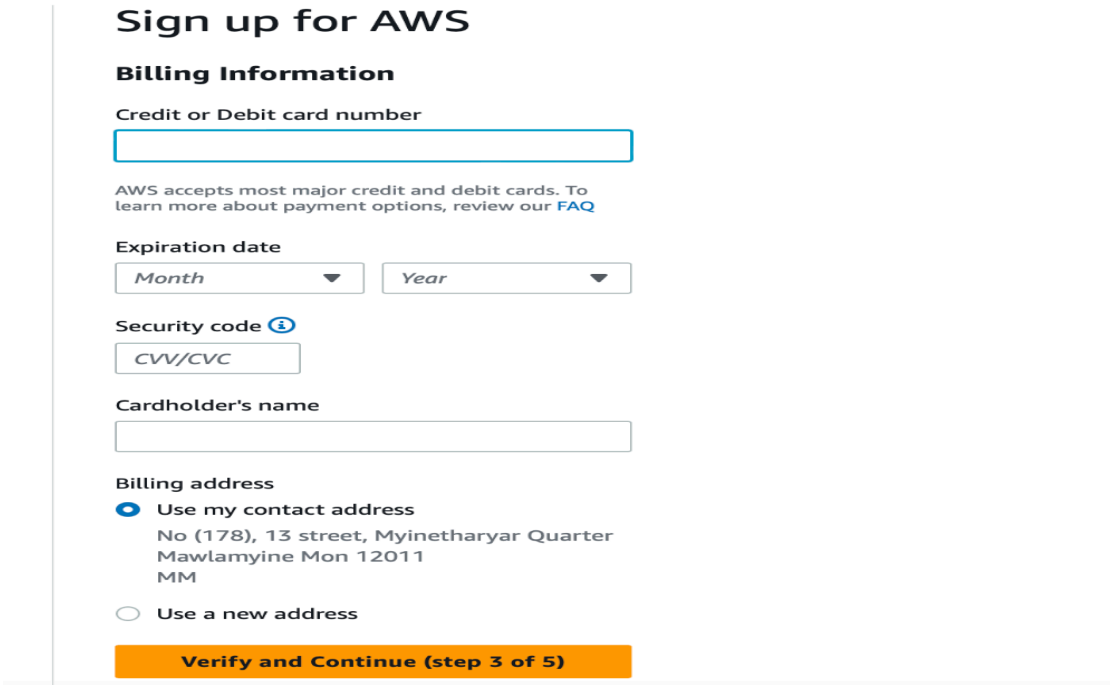


Figure 4.5. Creating AWS Account

According to Figure 4.6 make identity verification – Enter phone number and security check characters.

Figure 4.6. Creating AWS Account

Enter verification code that sent to SMS form AWS as shown in Figure 4.7.

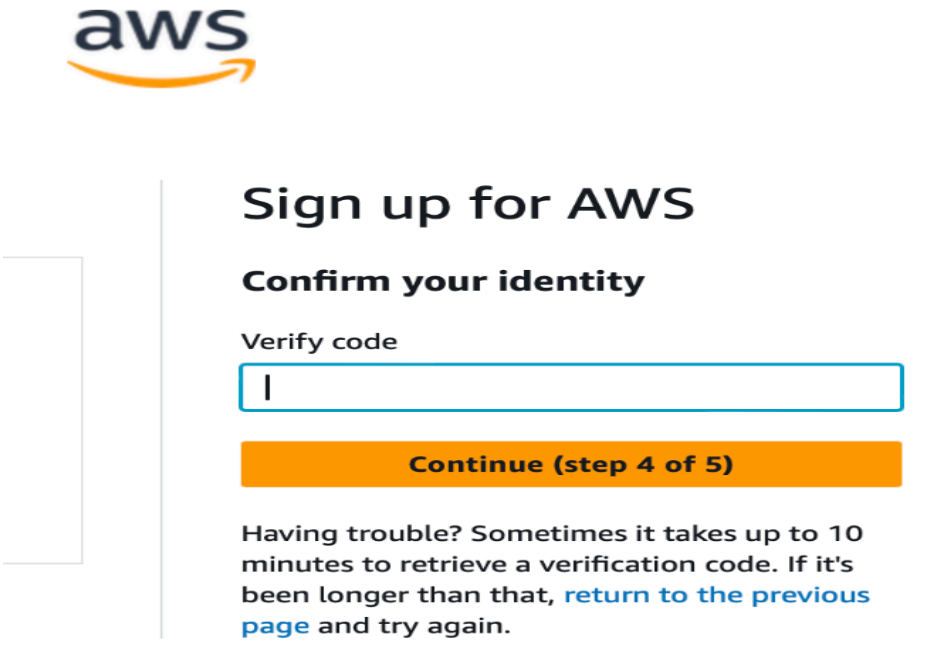


Figure 4.7. Creating AWS Account

Figure 4.8 shows to select a support plan and click “Complete Sign Up”.

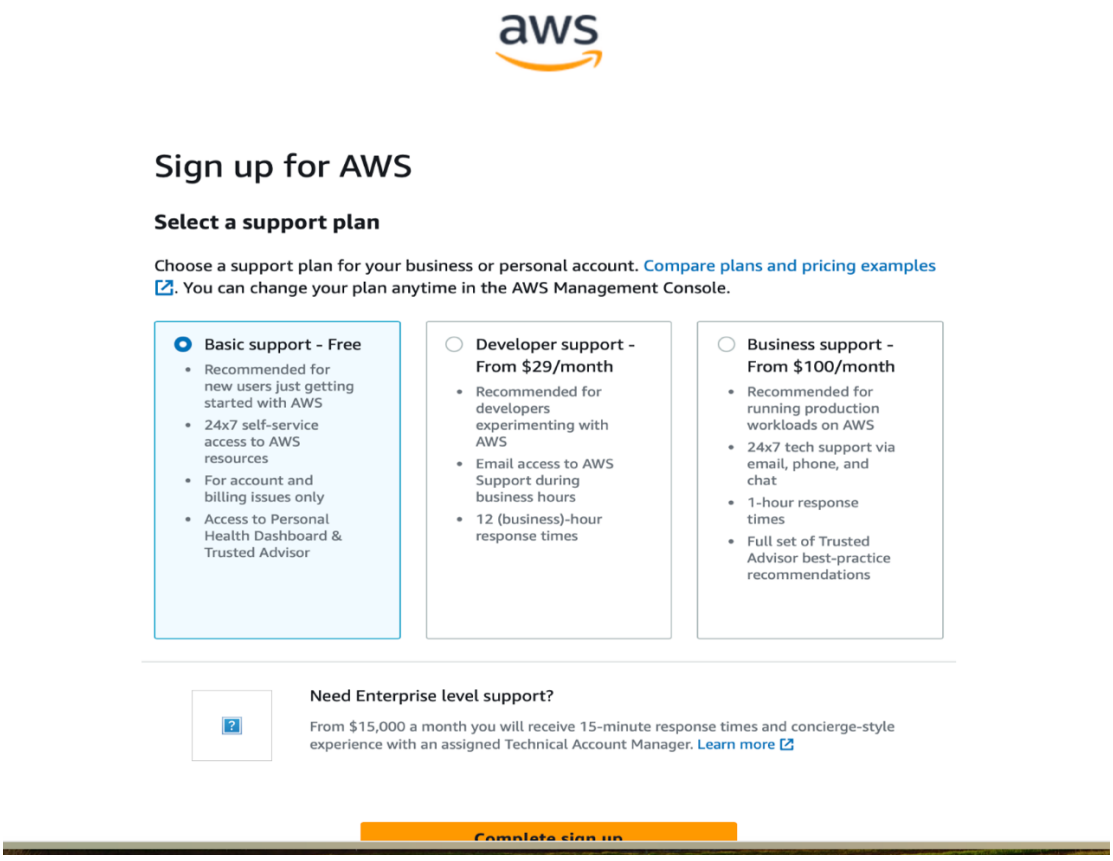


Figure 4.8. Creating AWS account

Figure 4.9 demonstrated, creating an AWS account is successfully completed and then click on “Go to the AWS Management Console” for sign up root user.

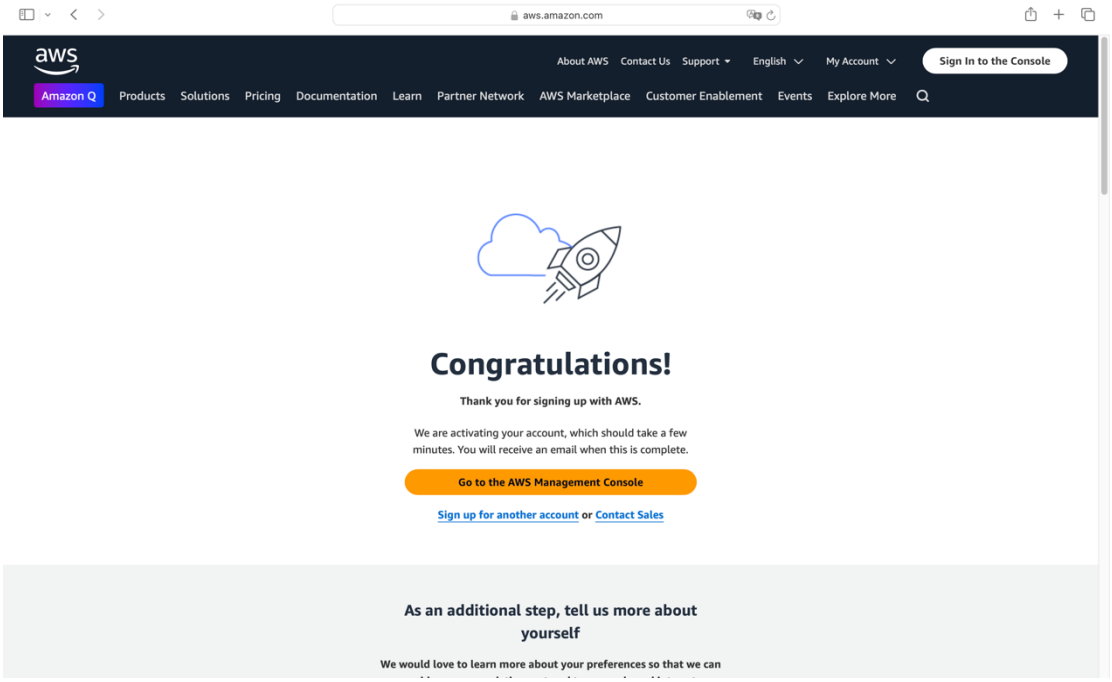


Figure 4.9. Creating AWS Account

Select Root user and fill up email as presented in Figure 4.10.

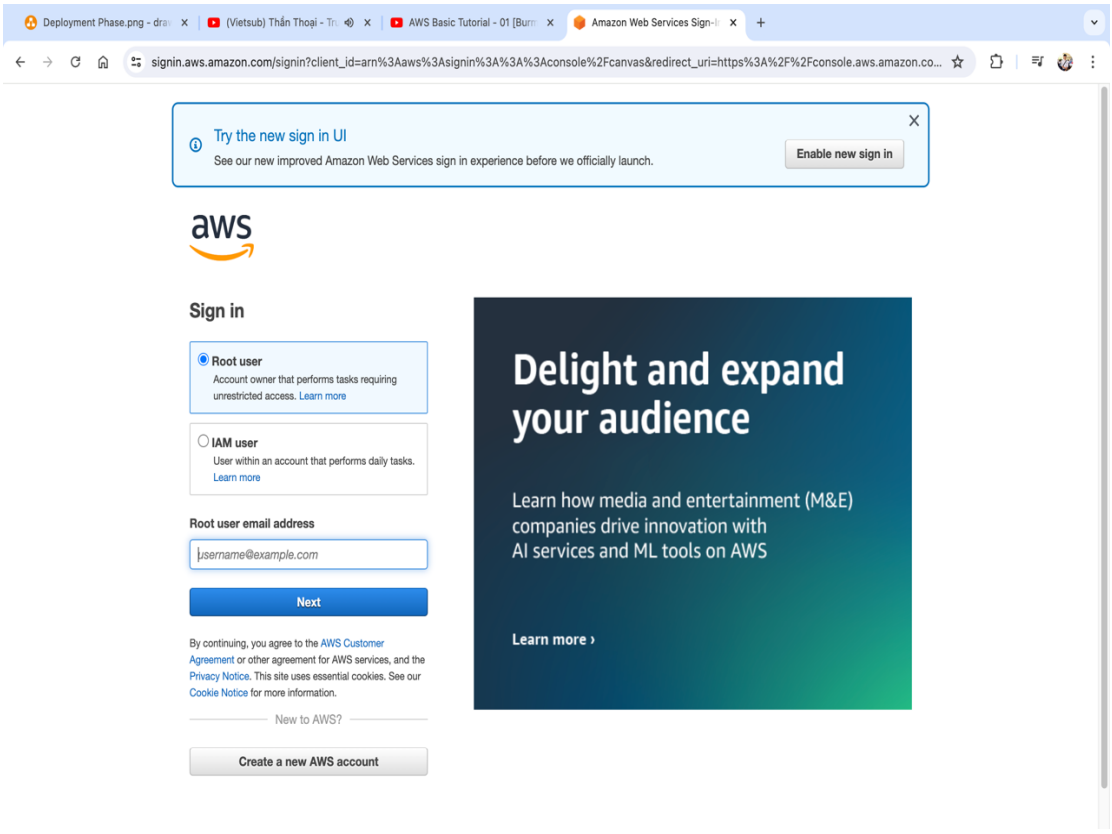


Figure 4.10. Sign up AWS Root User Account

Fill password for root user as shown in Figure 4.11.

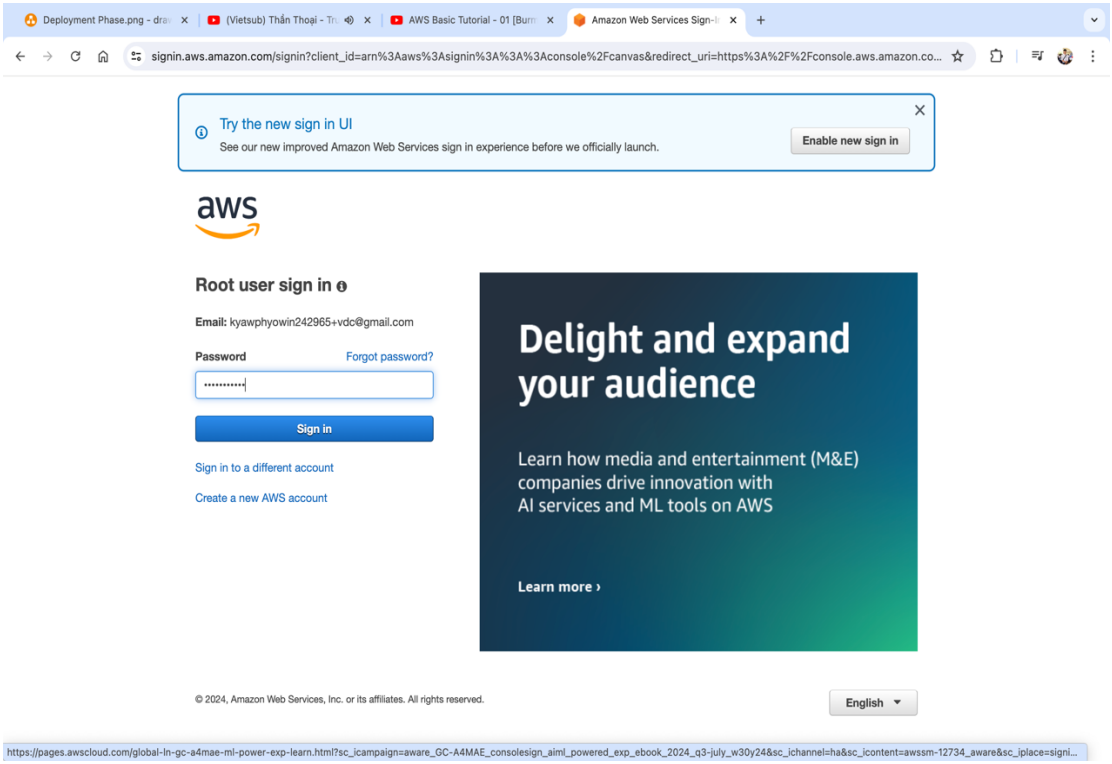


Figure 4.11. Sign up AWS Root User Account

Figure 4.12 displays the AWS management Console.

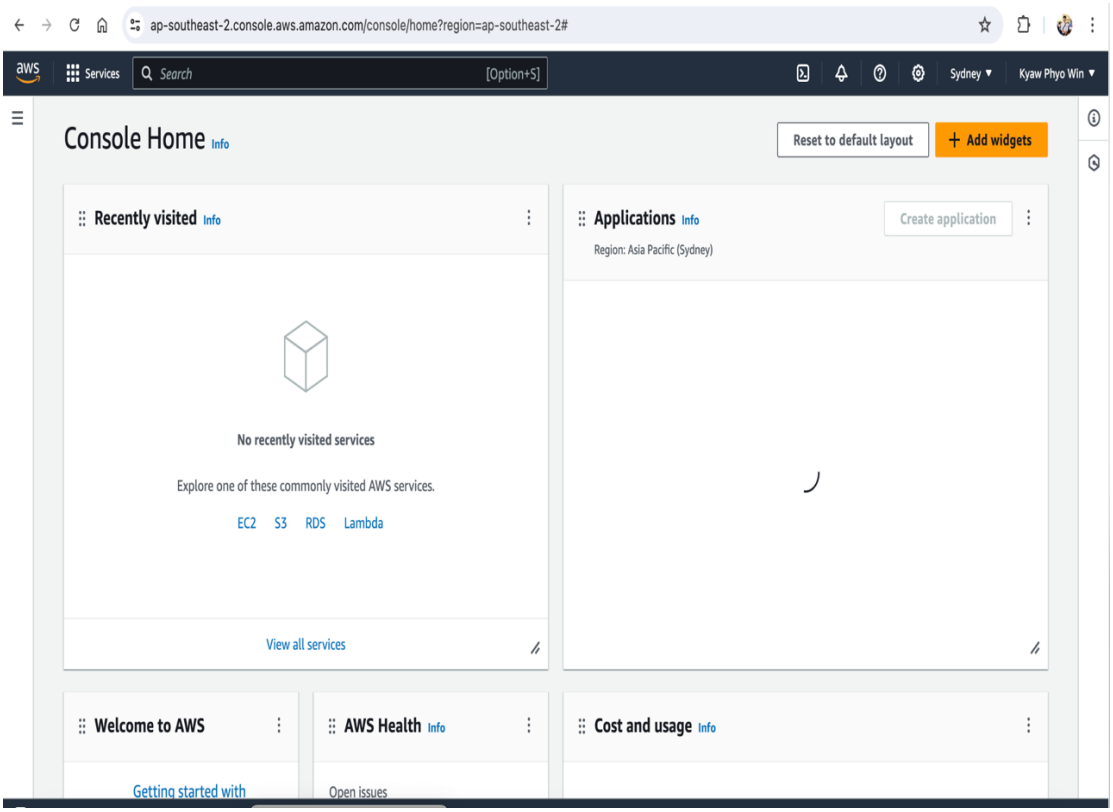


Figure 4.12. Sign up AWS Root User Account

4.3. Assign Multi-Factor Authentication (MFA) for Root User and Create Alias

Click on account name and select “Security credentials” as demonstrated in Figure 4.13.

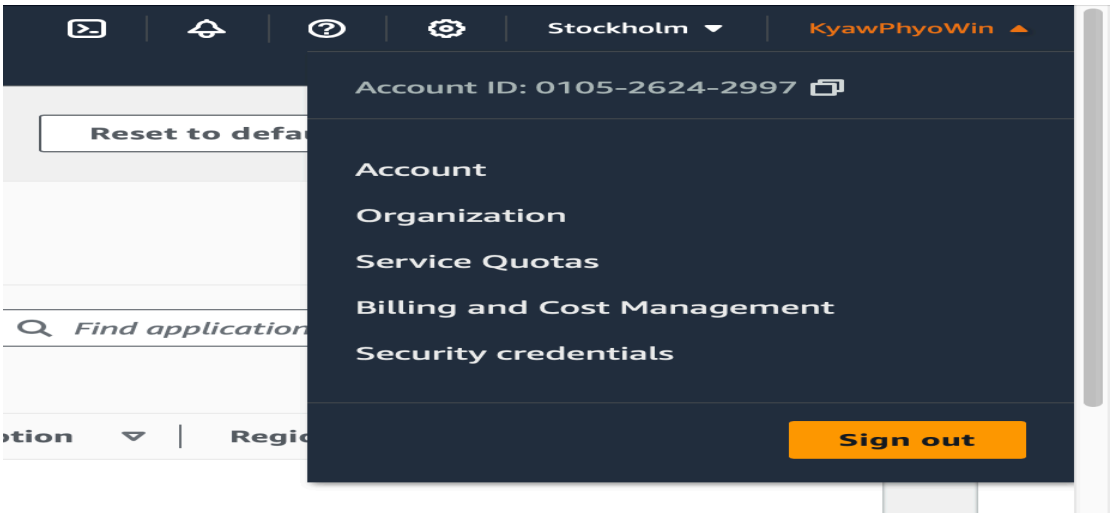


Figure 4.13. Assign MFA for Root User

Under “Multi-factor authentication”, click on “Assign MFA device” to create MFA for root user as shown in Figure 4.14.

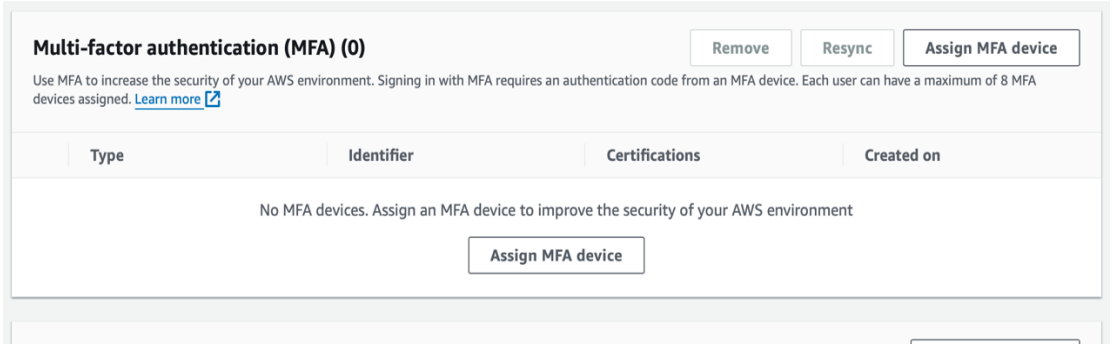


Figure 4.14. Assign MFA for Root User

According to Figure 4.15 enter device name that will be used within the identifying MFA for this device.

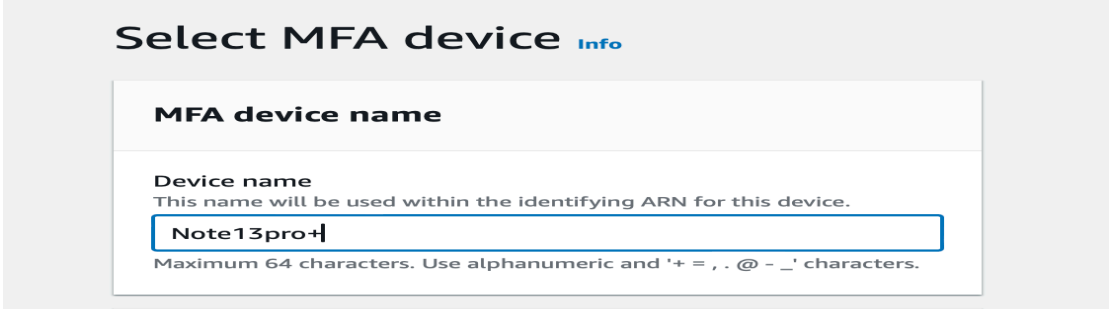


Figure 4.15. Assign MFA for Root User

As depicted in Figure 4.16, choose Authenticator app among the option devices and install authenticator app like Google authenticator, Authy, Duo mobile on device or computer.

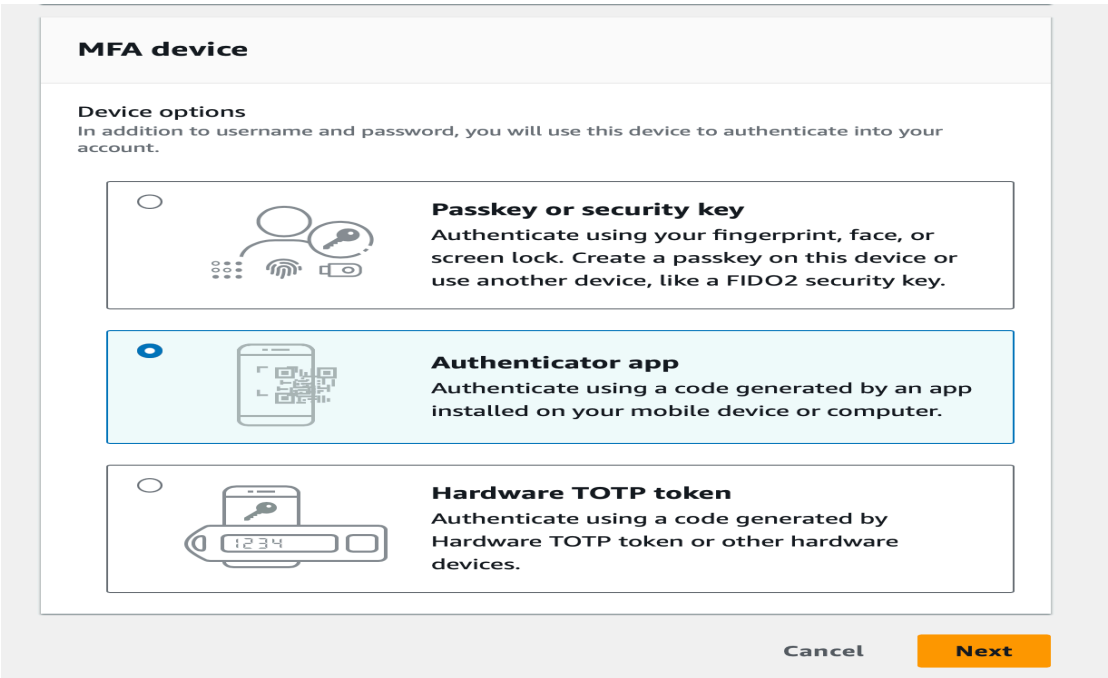


Figure 4.16. Assign MFA for Root User

Open authenticator app, scan the code and fill two consecutive MFA code, then click on “Add MFA” as presented in Figure 4.17.

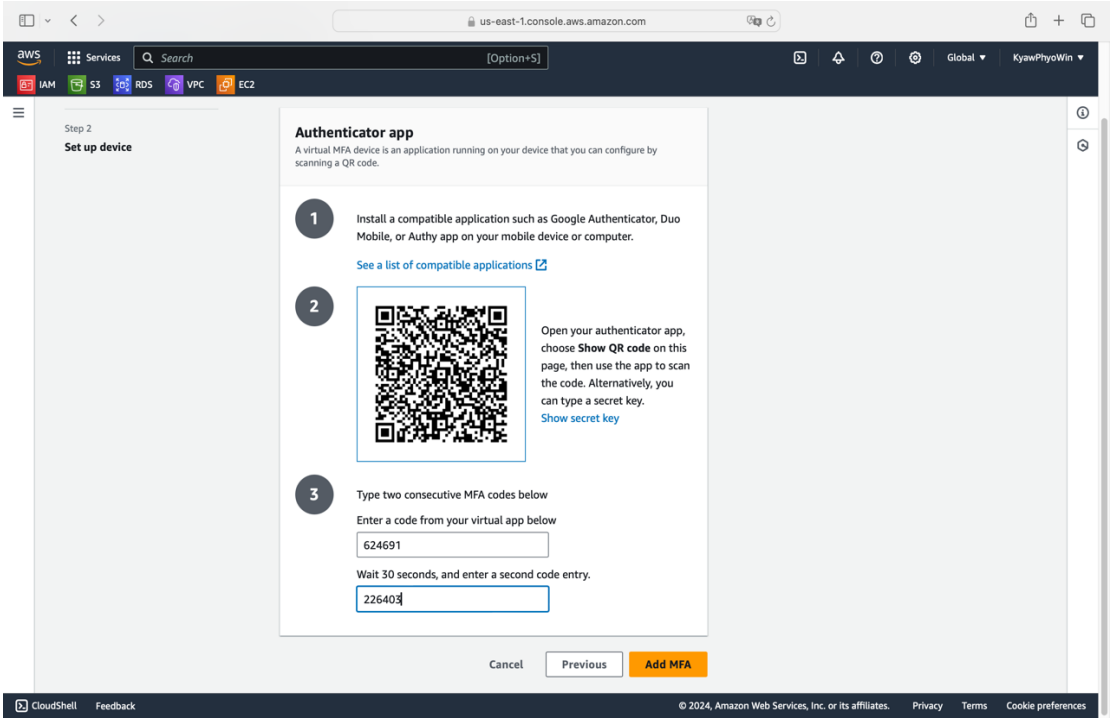


Figure 4.17. Assign MFA for Root User

According to the Figure 4.18 assign MFA device for root user completed successfully.

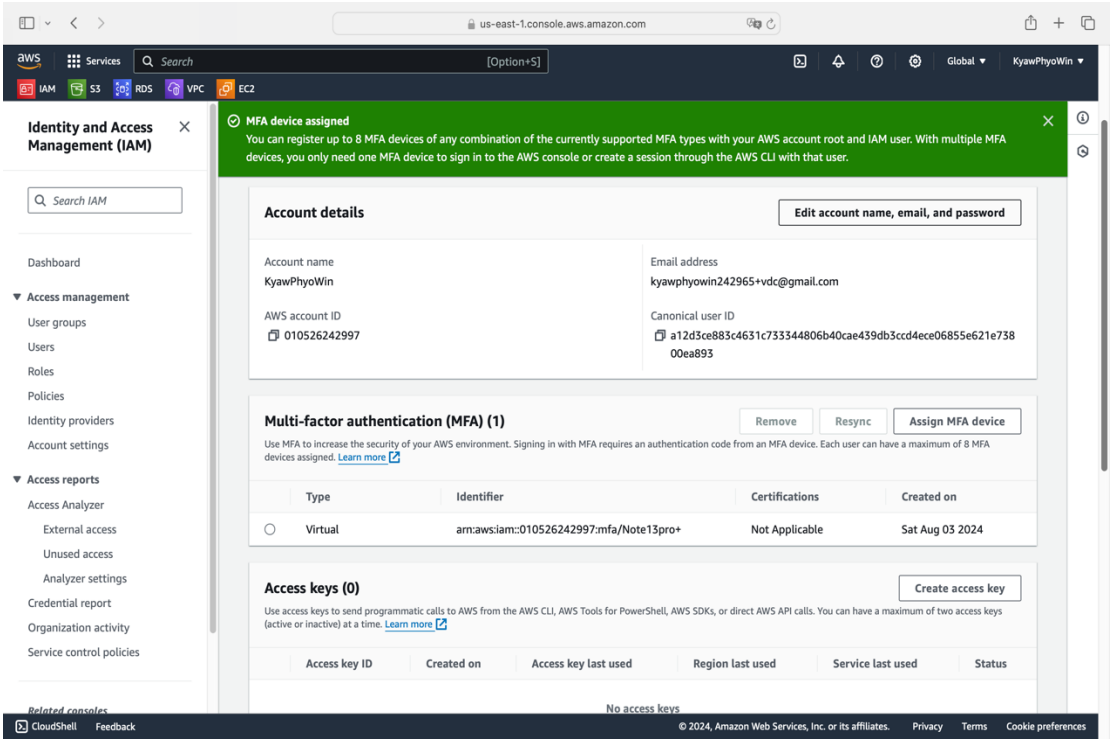


Figure 4.18. Assign MFA for Root User

Select Dashboard at the left navigation bar and click on “Create” under the Account Alias at the right screen as shown in Figure 4.19.

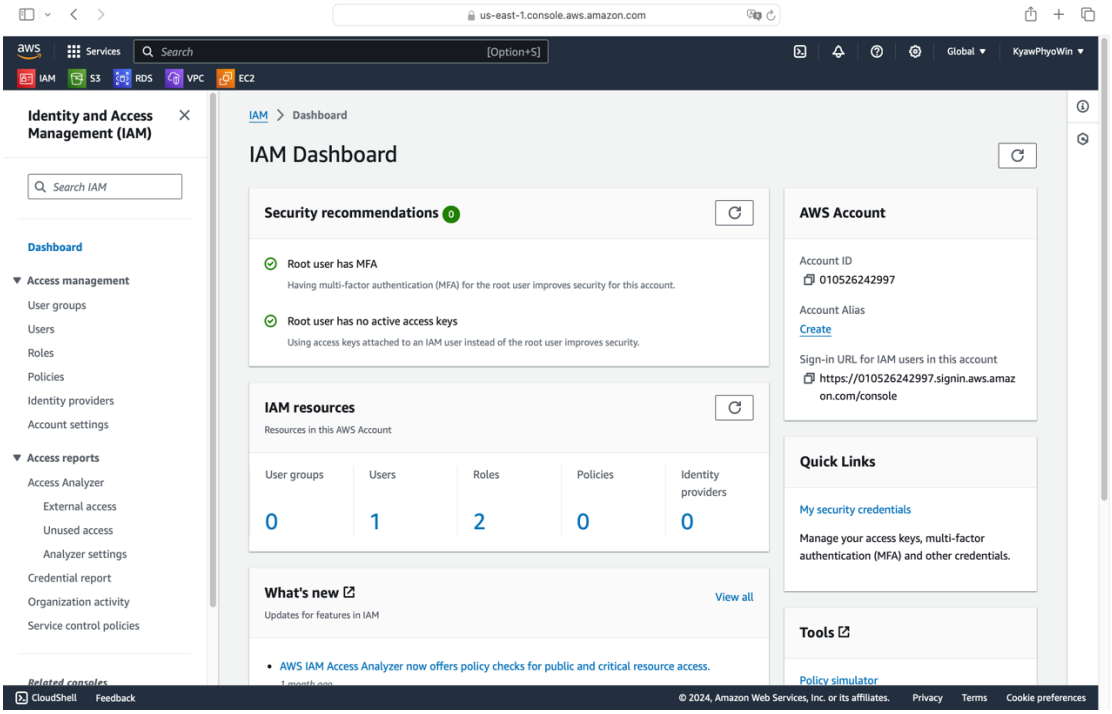


Figure 4.19. Create Account Alias

Enter preferred alias and click on “Create alias” as demonstrated in Figure 4.20.

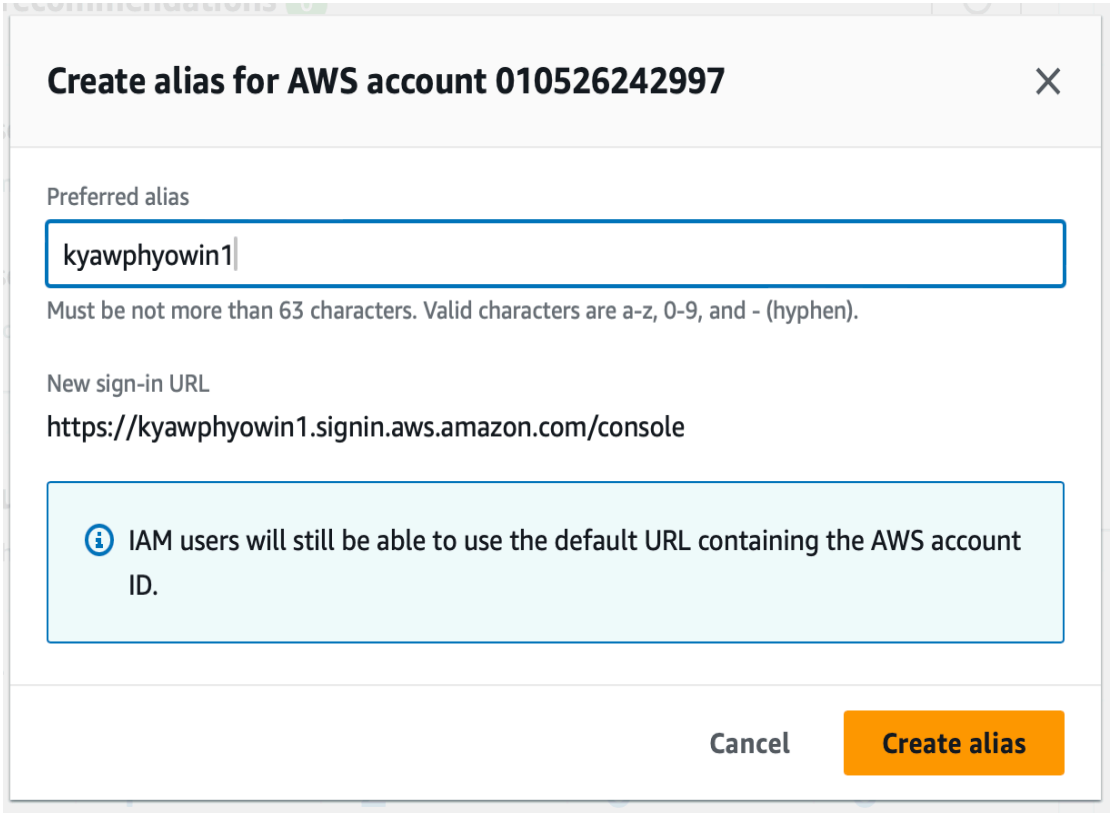


Figure 4.20. Create Account Alias

Figure 4.21 shows alias creation is completed successfully.

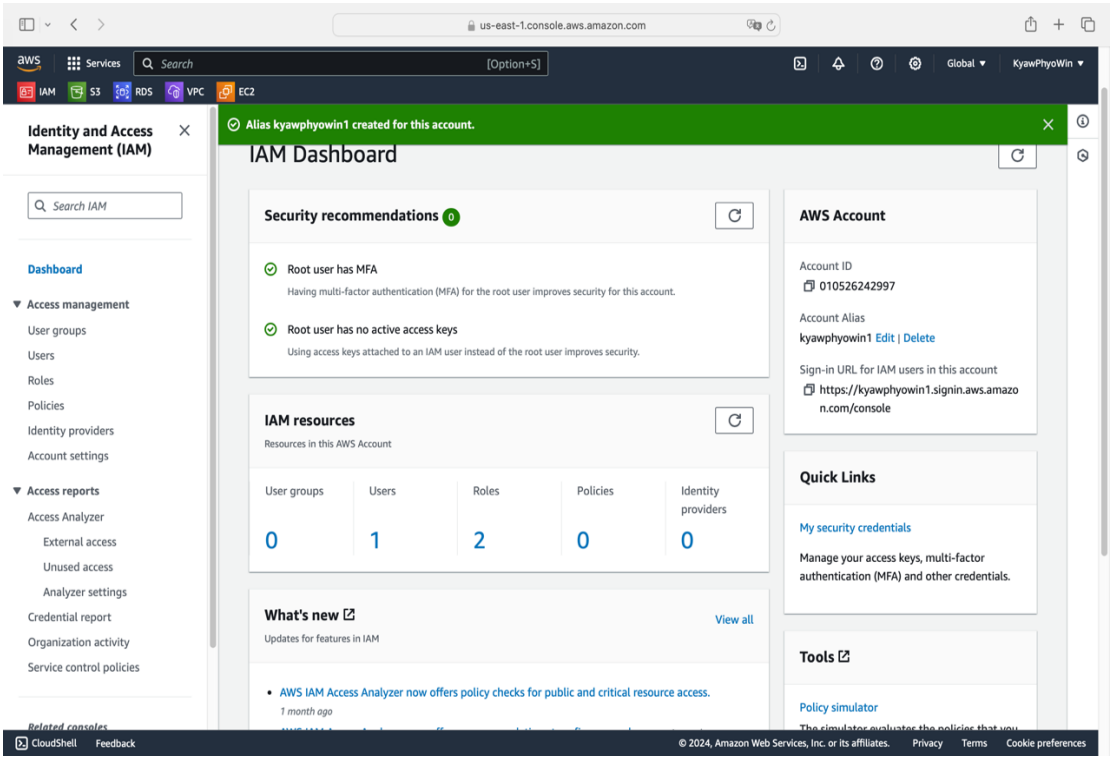


Figure 4.21. Create Account Alias

4.4. Create IAM User, Assign MFA for IAM User and Sign Up

As presented in Figure 4.22 navigate to the IAM Dashboard. In the IMA Dashboard, click on “Users” in the left navigation pane.

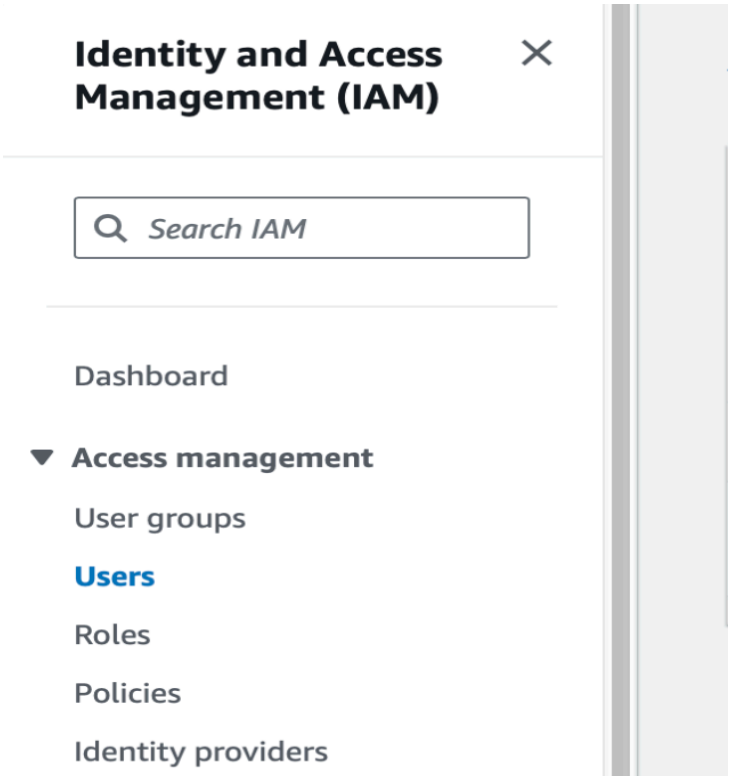


Figure 4.22. Creating IMA User

Click the “Create user” button as shown in Figure 4.23.

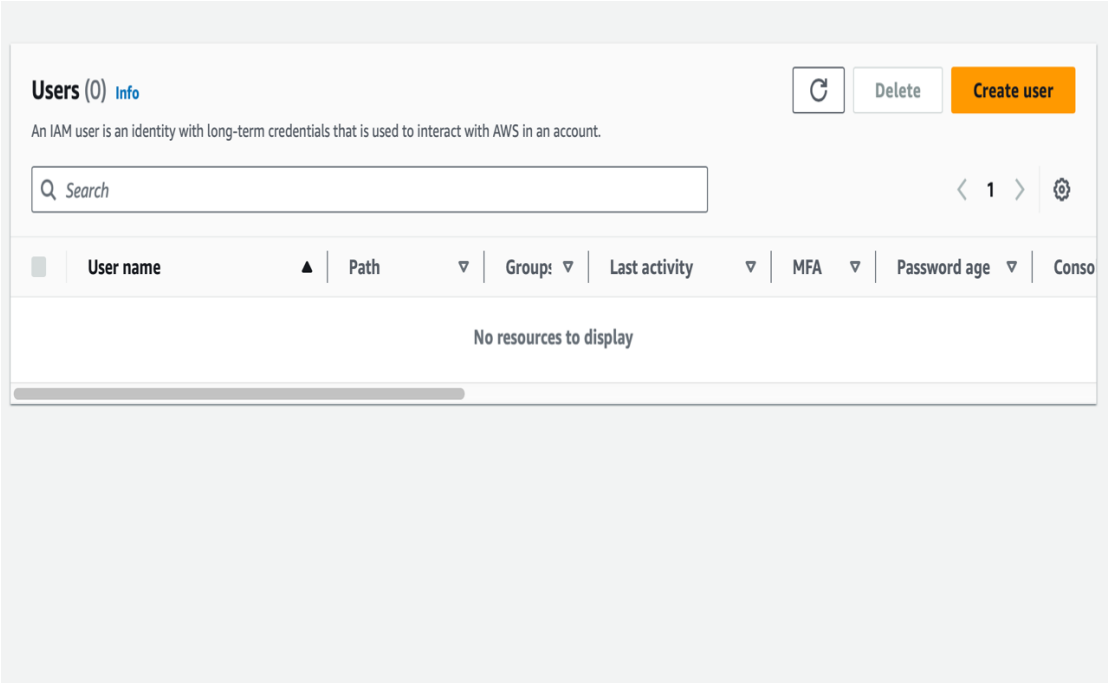


Figure 4.23. Creating IMA User

Figure 4.24 presents to specify user details, enter user name, check on “Provide user access to the AWS Management and select on “I want to create an IAM user”.

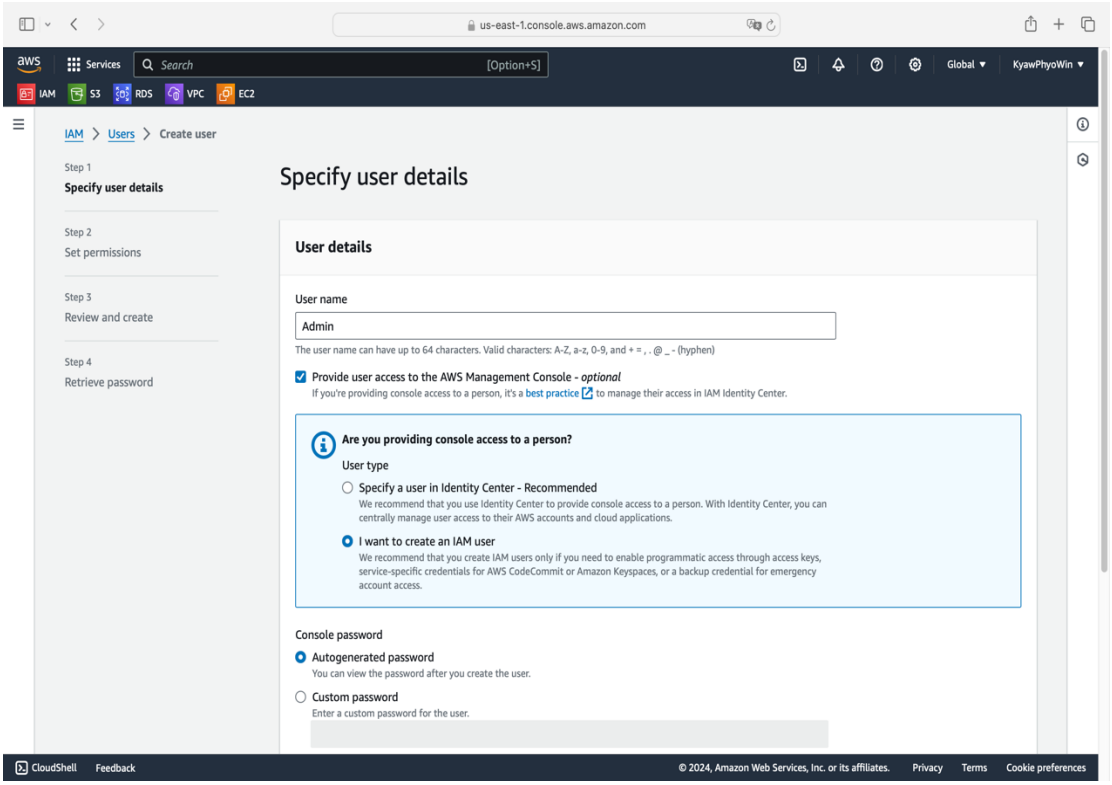


Figure 4.24. Creating IMA User

As displayed in Figure 4.25 select on “Custom password” and fill password for IAM user.

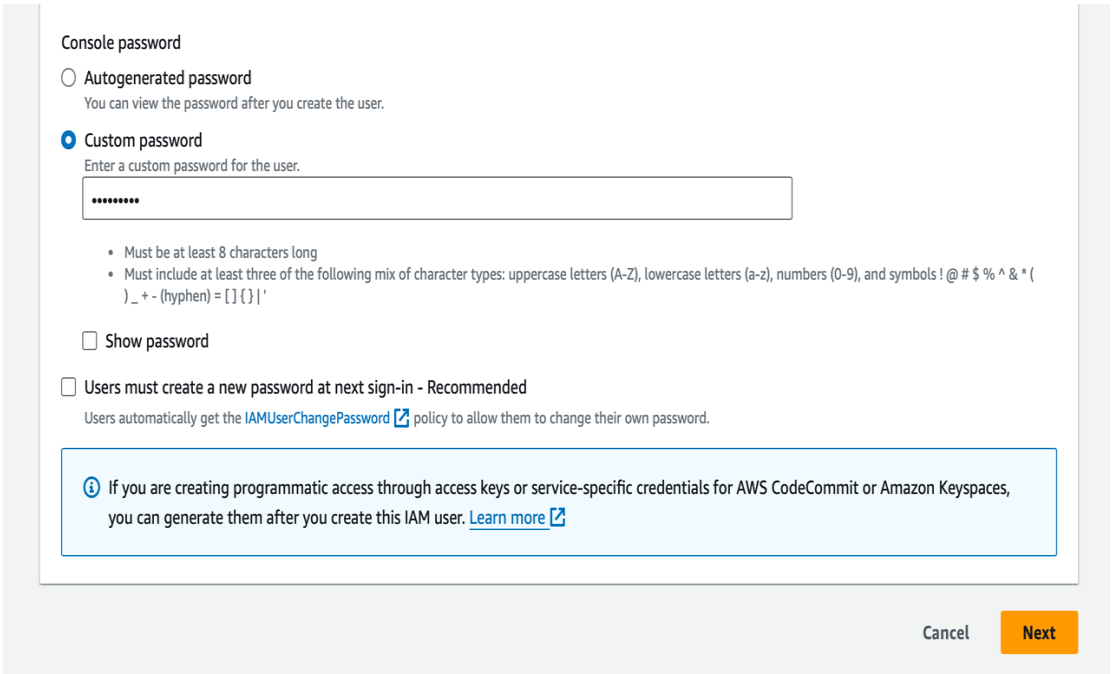


Figure 4.25. Creating IMA User

According to Figure 4.26 choose “Attach policies directly” to attach one or more managed or customer managed policies to the user to set permissions for IAM user.

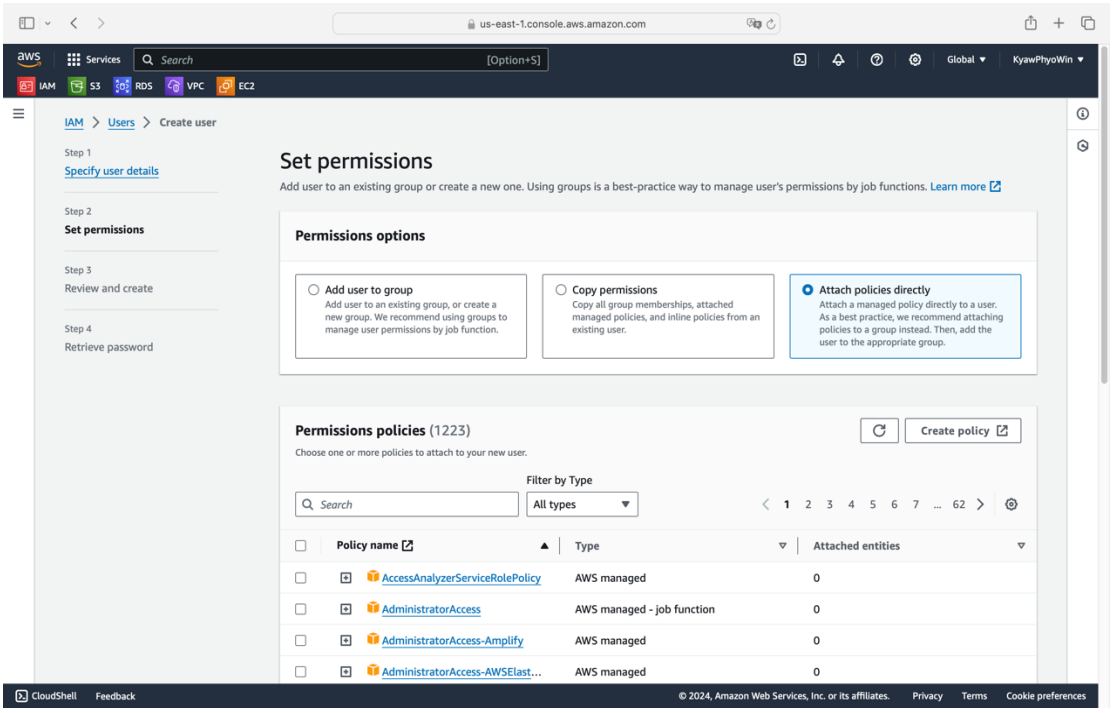


Figure 4.26. Creating IMA User

And then, search for and select the appropriate policies for the IAM user and click on “Next” as presented in Figure 4.27.

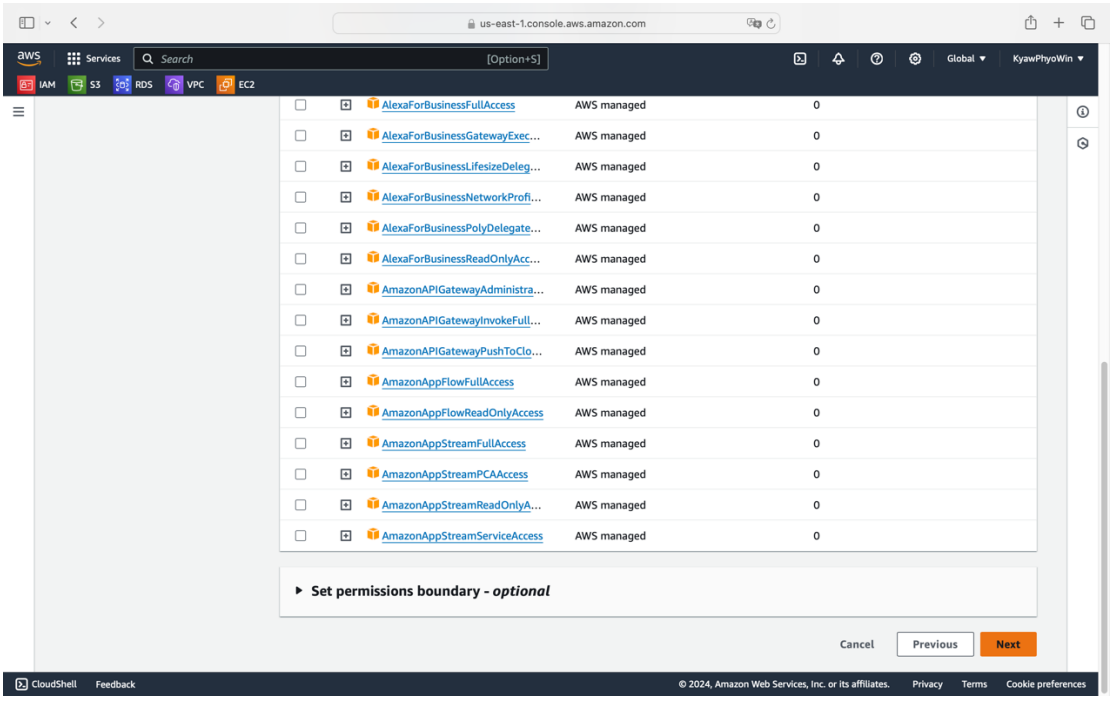


Figure 4.27. Creating IMA User

Figure 4.28 shows review of the user details, and permissions and click the "Create user" button.

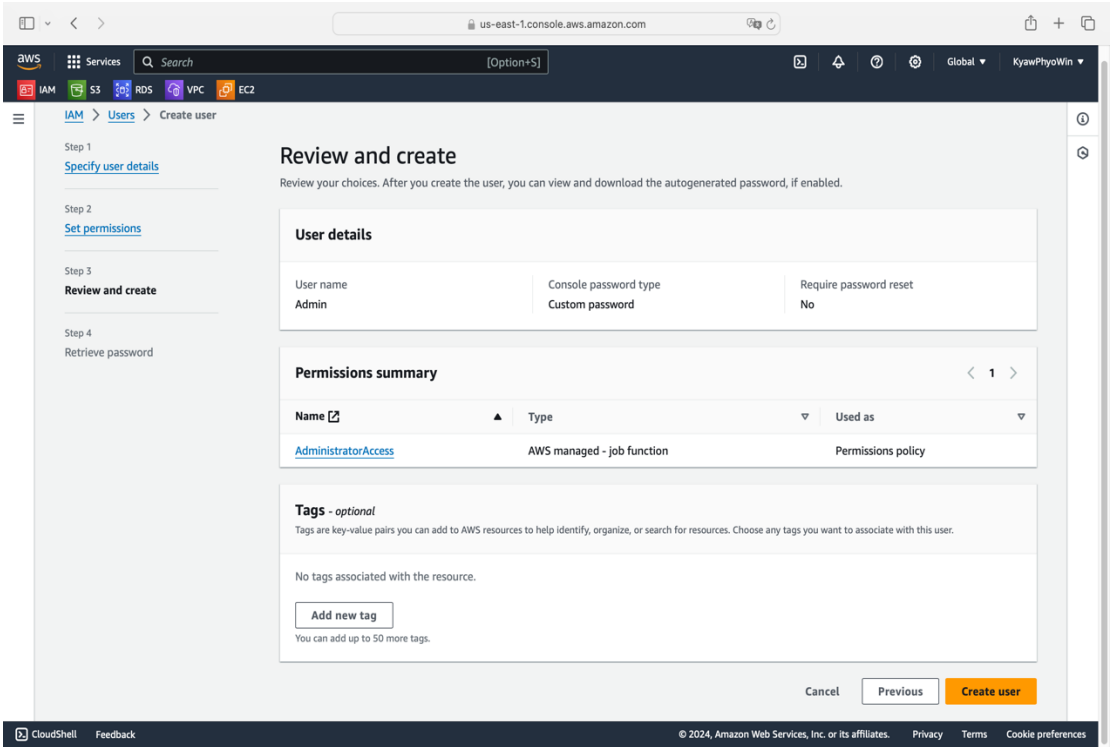


Figure 4.28. Creating IMA User

IAM user creation is completed successfully as depicted in Figure 4.29.

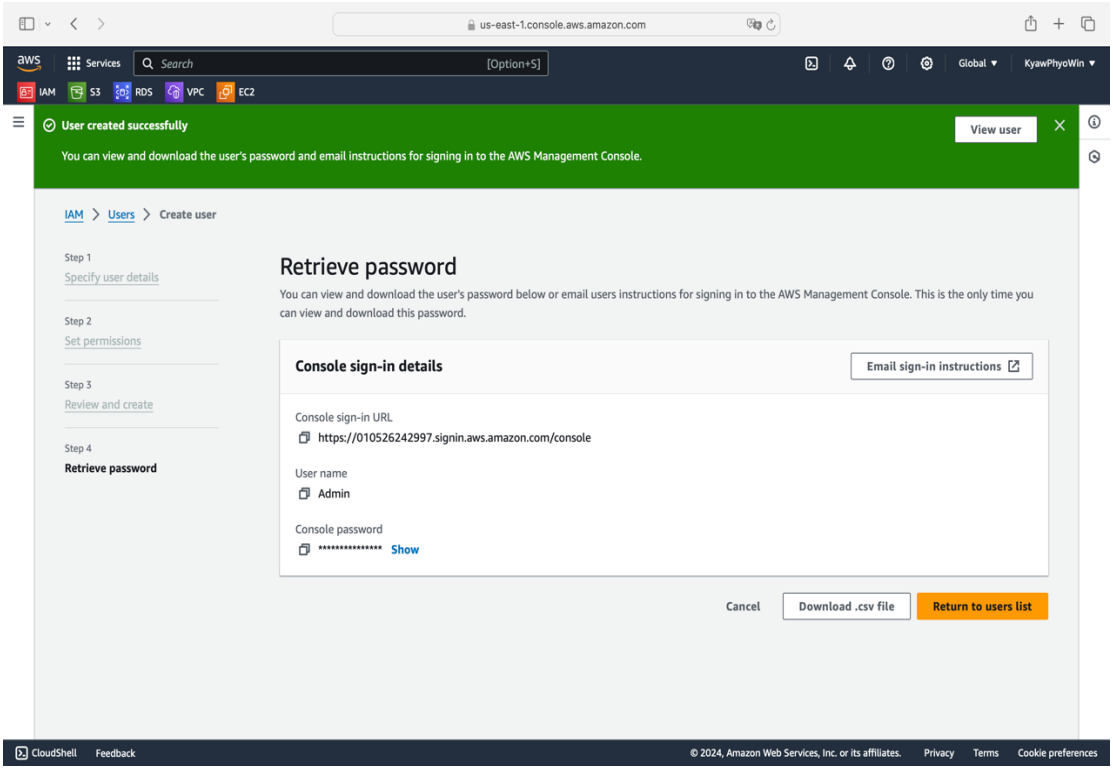


Figure 4.29. Creating IMA User

For added security, enable MFA for the user, go to the IAM Dashboard, select “User”. choose the user, go to the “Security credentials” tab, and click under the “Multi-factor authentication (MFA)” section as demonstrated in Figure 4.30.

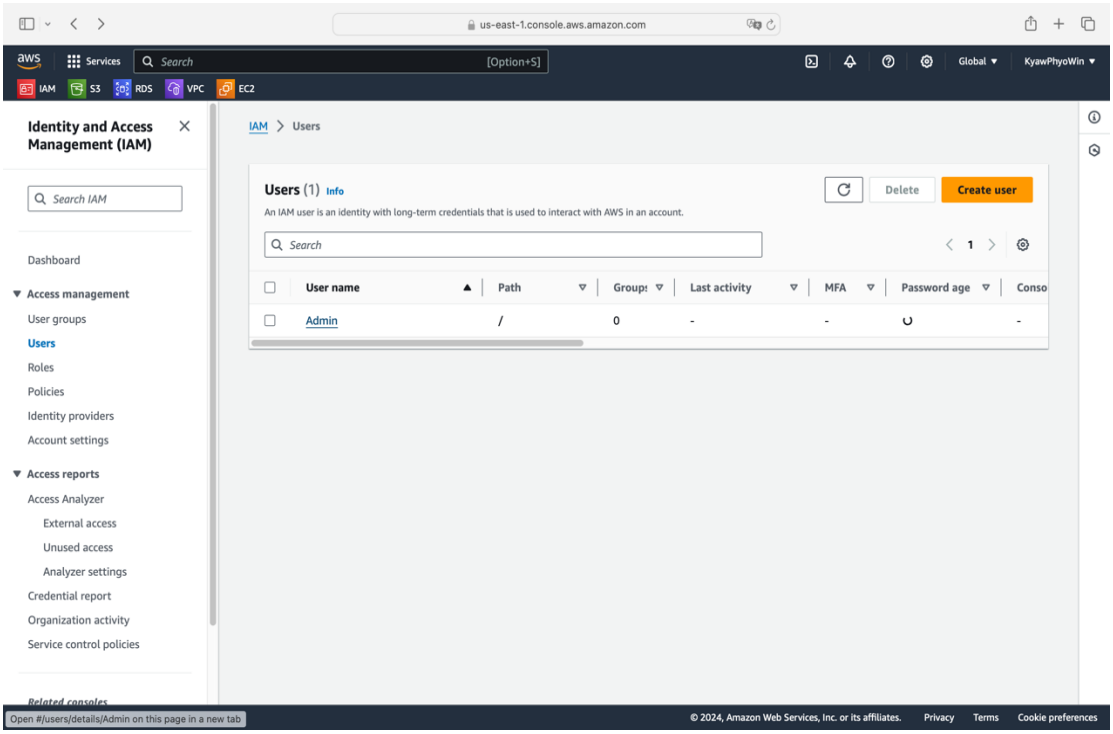


Figure 4.30. Assign MFA for IMA User

Choose the user, go to the “Security credentials” tab, and click under the “Multi-factor authentication (MFA)” section as shown in Figure 4.31. And then follow the steps to assign an MFA devices just like for the root user.

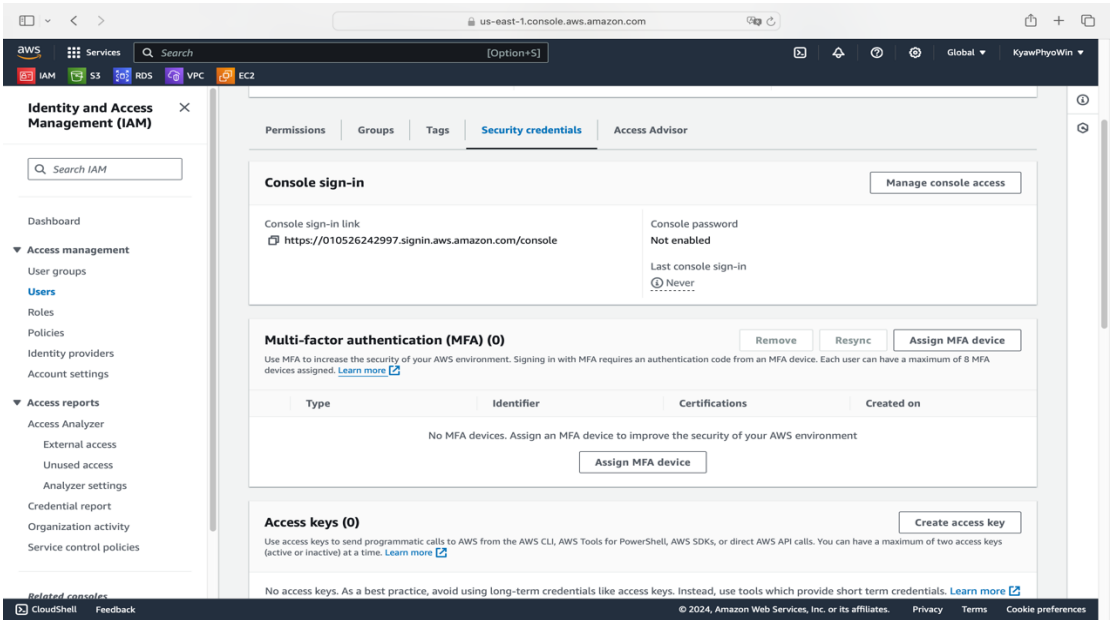


Figure 4.31. Assign MFA for IMA User

Figure 4.32 demonstrates to verify MFA set up sign out the root user and sign in back using the IAM user's credentials. Select IMA user and enter account alias.

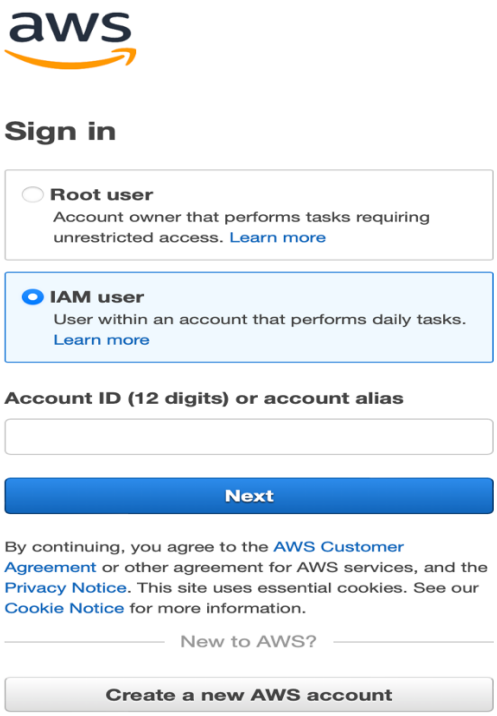


Figure 4.32. Verify MFA as IAM User

Enter IAM user name, password and click the "Sign in" button as presented in Figure 4.33.

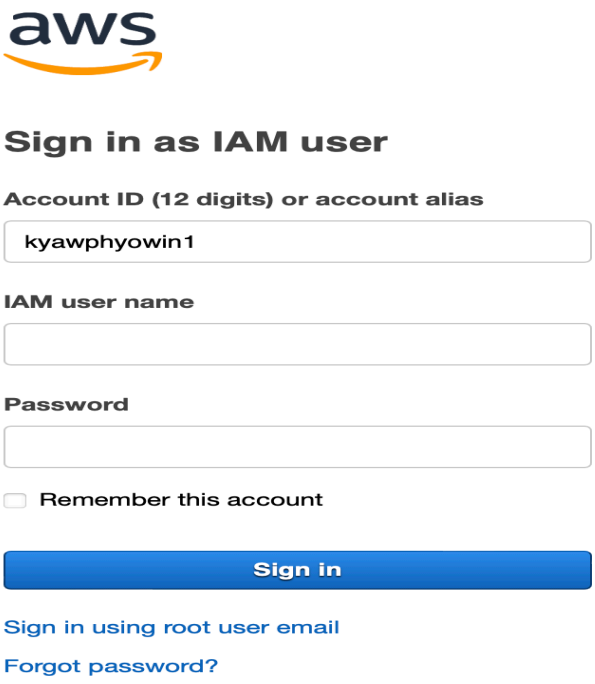


Figure 4.33. Verify MFA as IAM User

Enter an MFA code form authenticator on device as displayed in Figure 4.34.

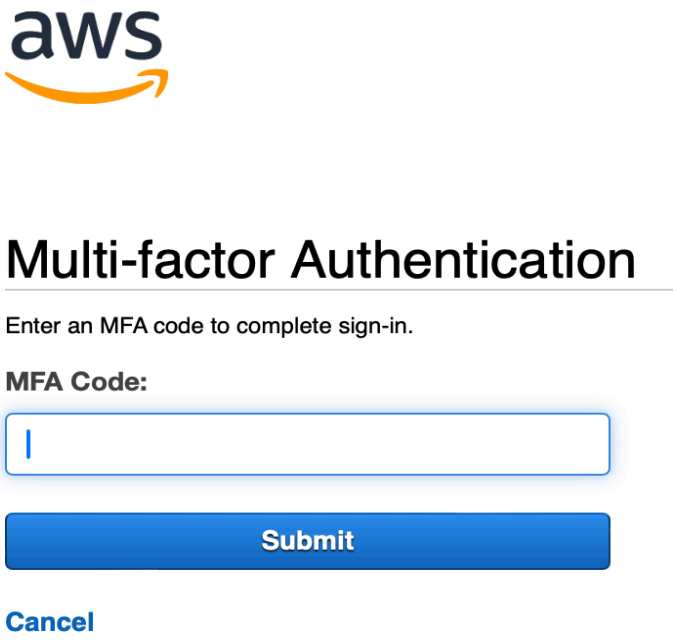


Figure 4.34. Verify MFA as IAM User

Figure 4.35 shows access the AWS Console home as a IAM user.

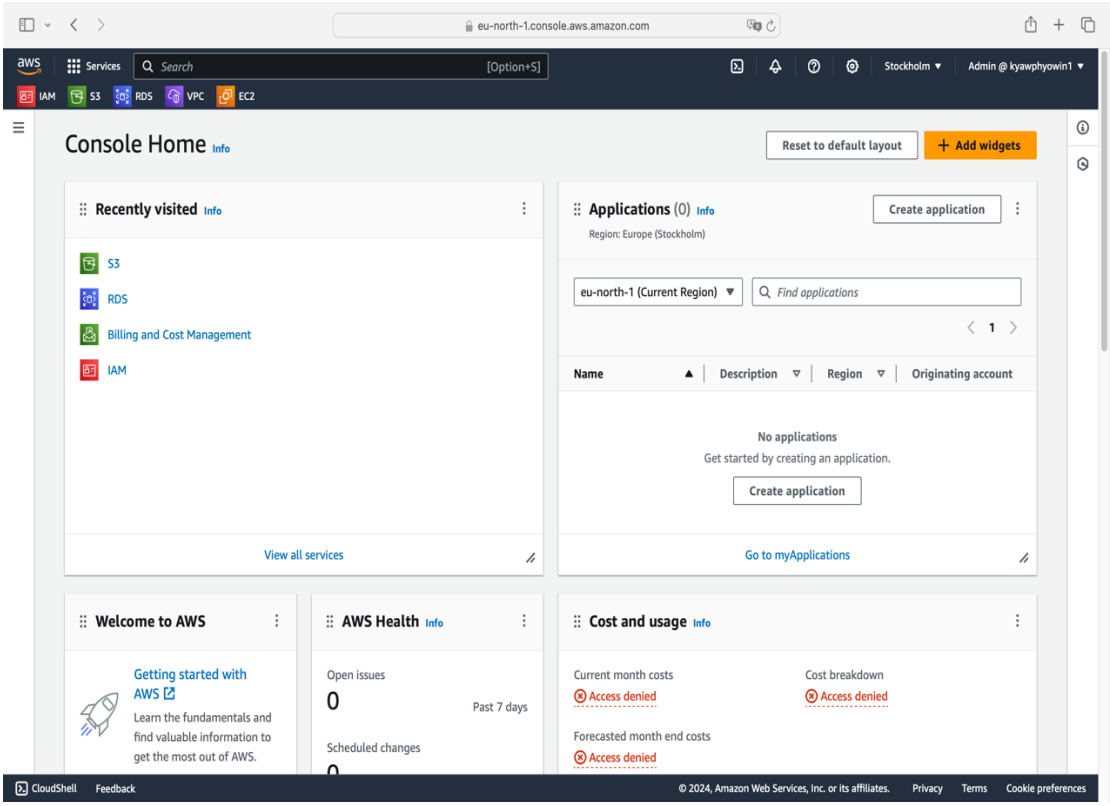


Figure 4.35. Verify MFA as IAM User

4.5. Sequential Guide to Configure S3 (Simple Storage Service)

Navigate to the S3 services and click on “Create bucket” as shown in Figure 4.36.

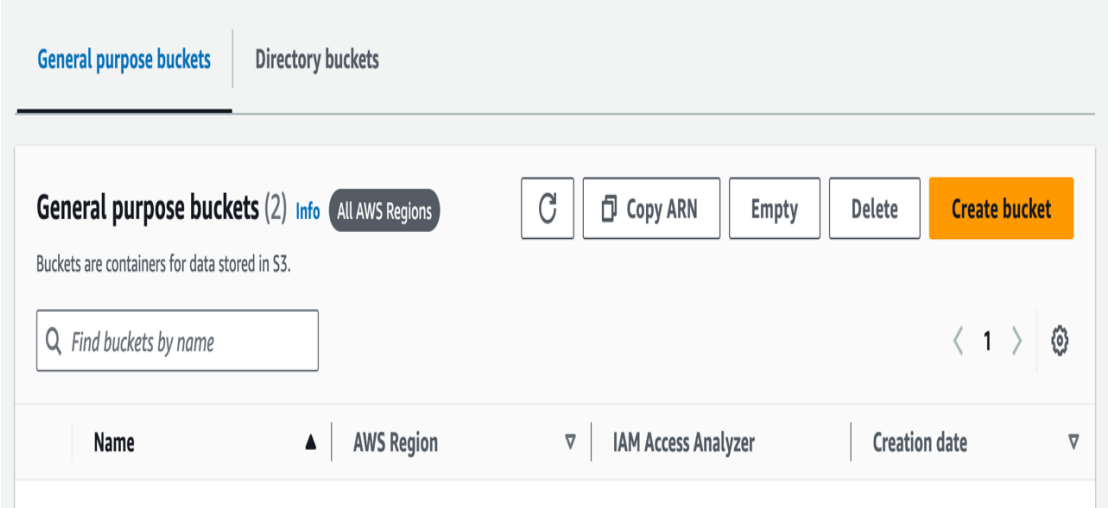


Figure 4.36. Configure S3

As presented in Figure 4.37 choose bucket type, select a region close to your data center and enter a unique bucket name.

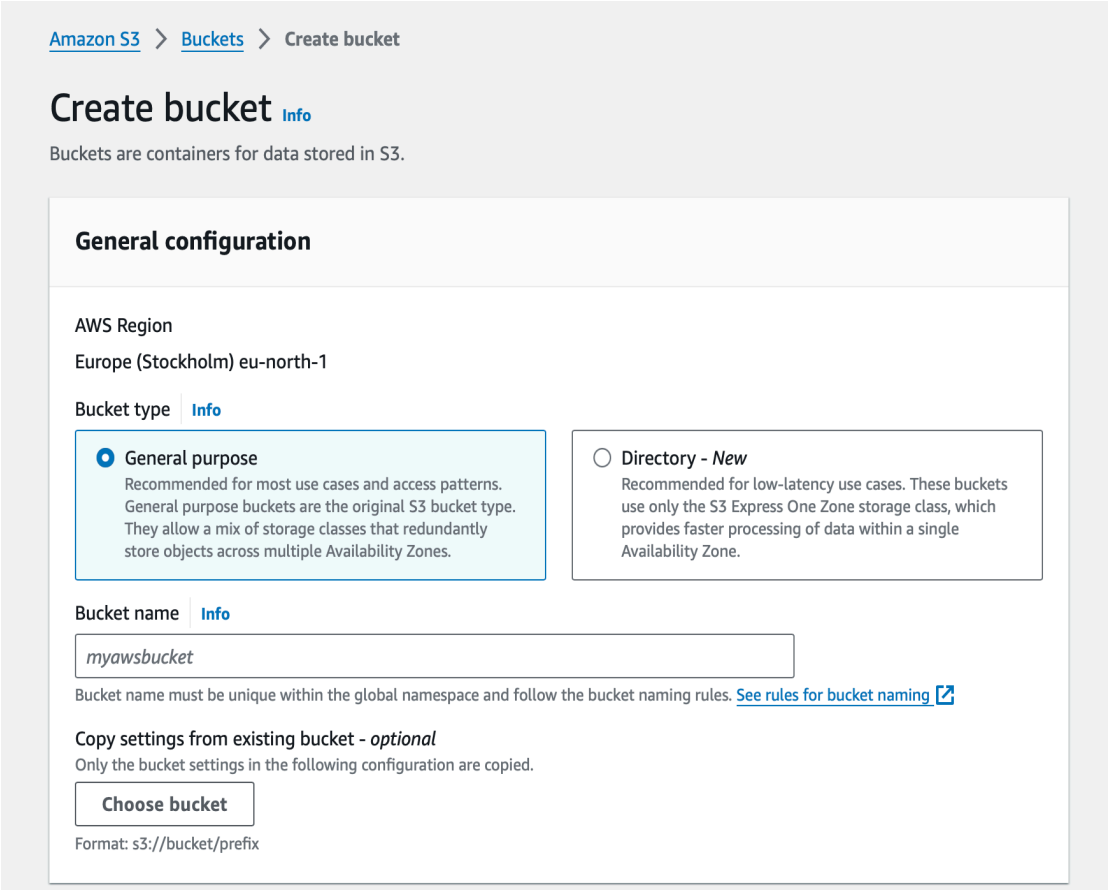


Figure 4.37. Configure S3

Choose object ownership and uncheck block all public access as shown in Figure 4.38.

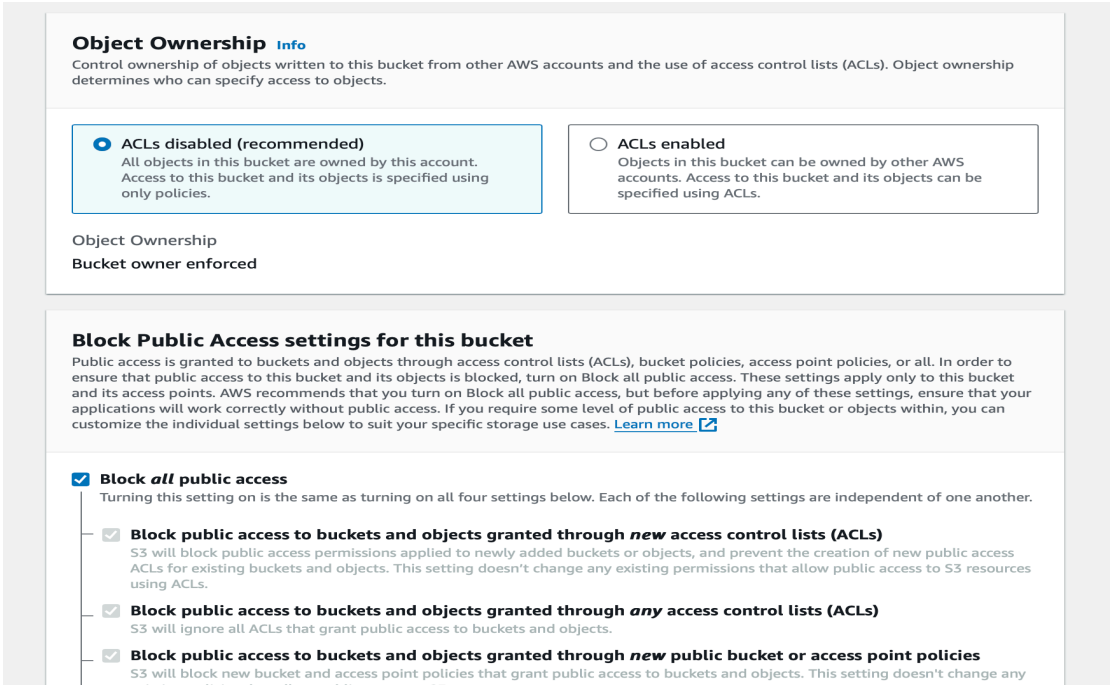


Figure 4.38. Configure S3

Click on “Create bucket” button as presented in Figure 4.39.

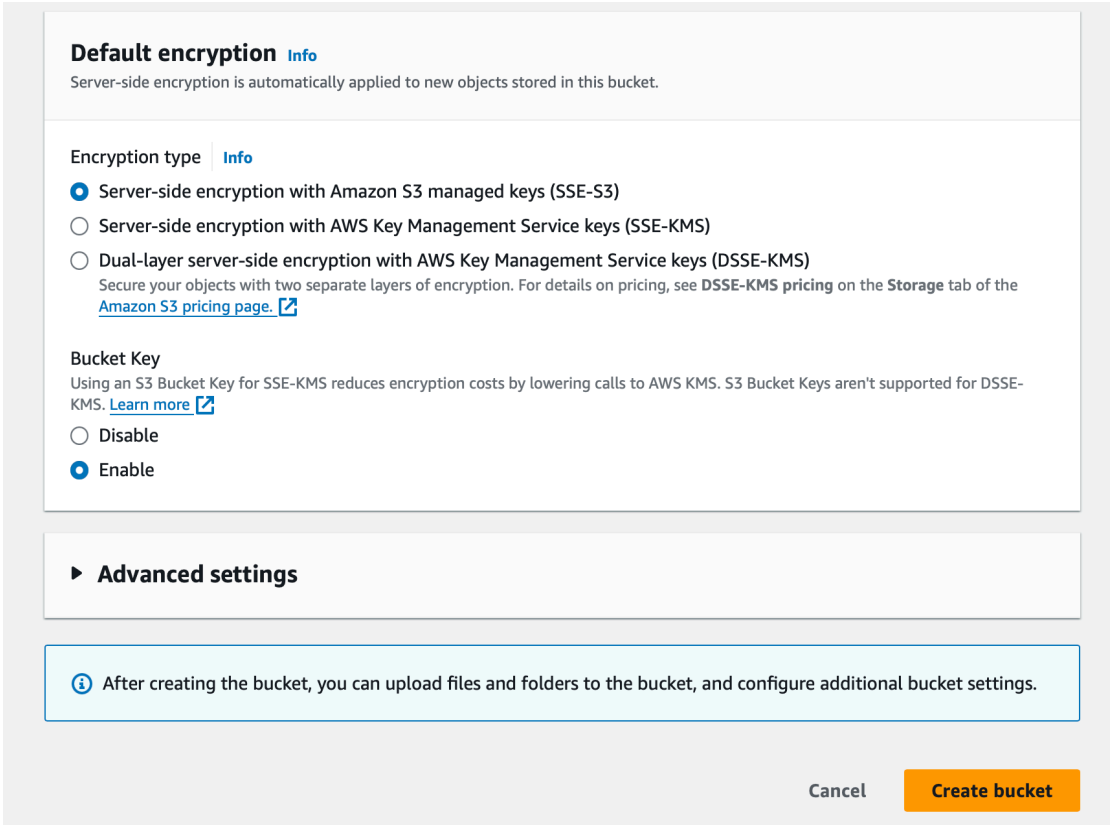


Figure 4.39. Configure S3

Figure 4.40 presents Amazon S3 bucket and click on the bucket name to add permission for bucket.

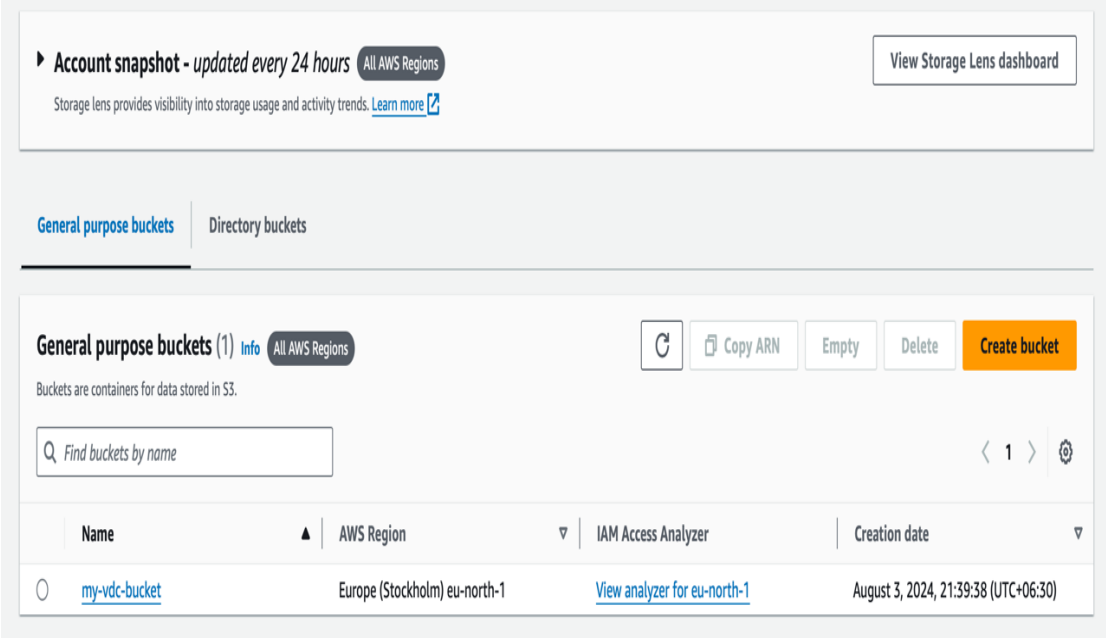


Figure 4.40. Configure S3

As demonstrated in Figure 4.41 go to “Permissions’ tab and scroll down.

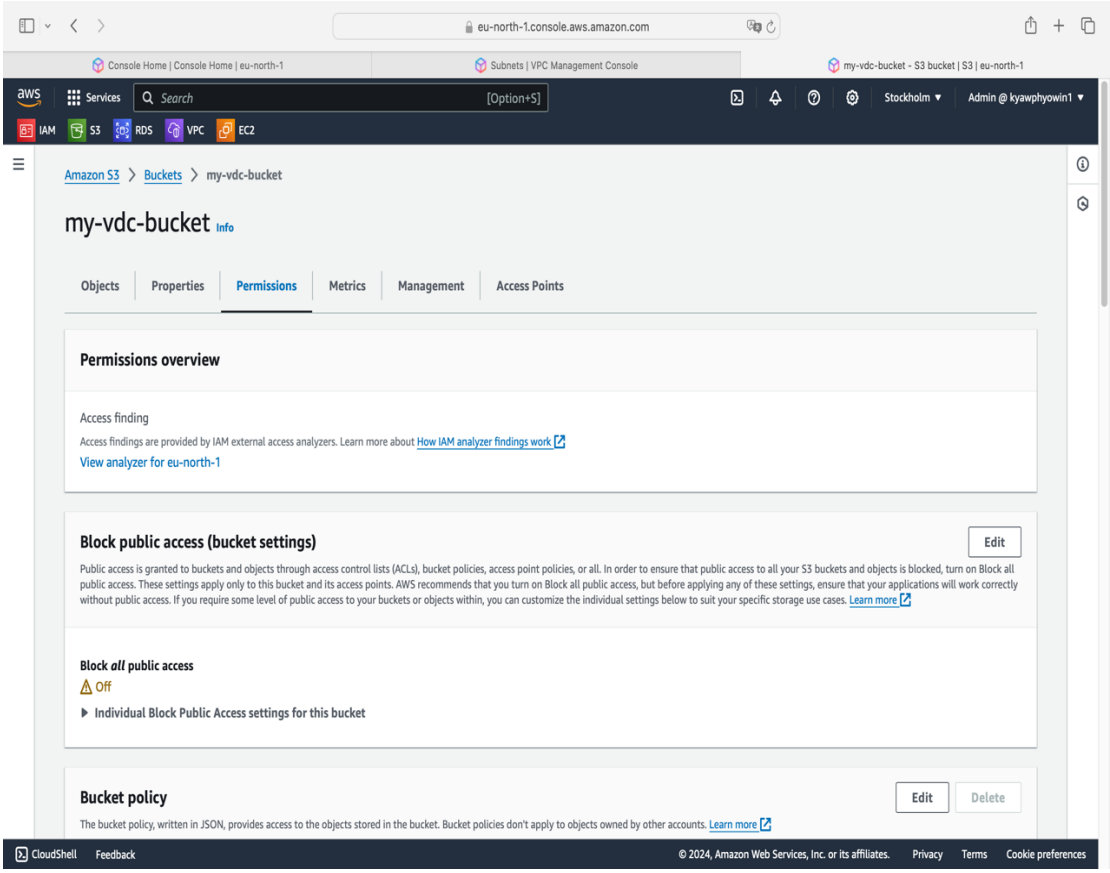


Figure 4.41. Configure S3

Click “Edit” button on bucket policy as depicted in Figure 4.42.

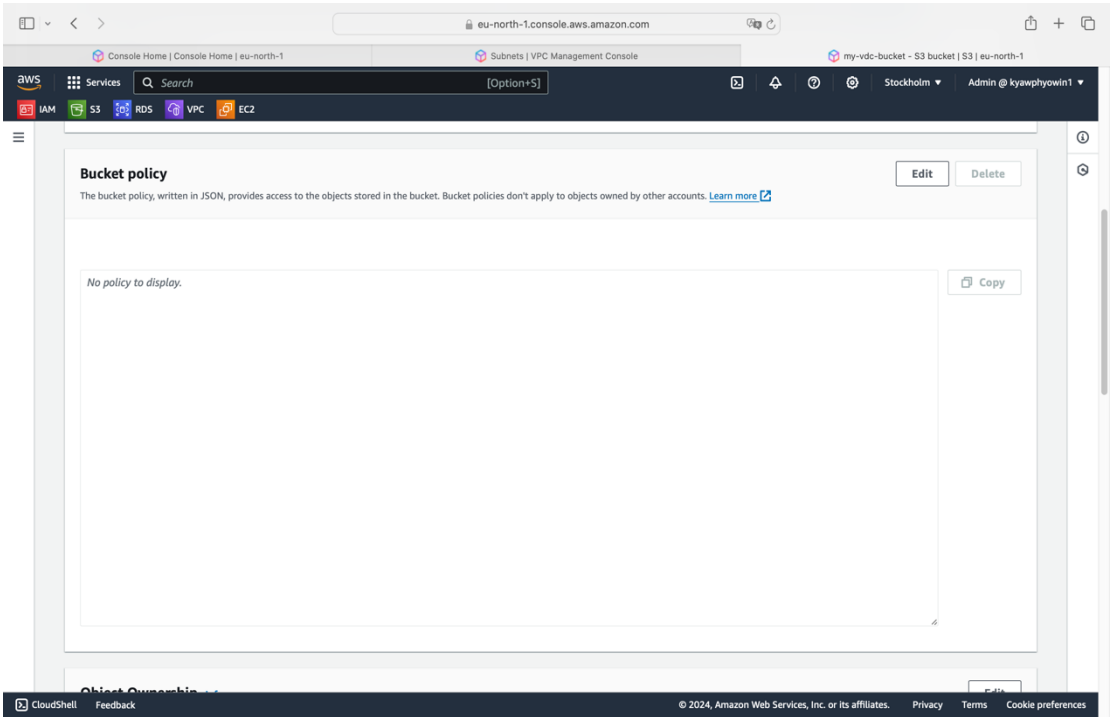


Figure 4.42. Configure S3

Figure 4.43 presented policy script to grand public read access to S3 and then click on “Save change” button.

Figure 4.43. Configure S3

As evidenced by Figure 4.44 S3 configuretion is successfully complete.

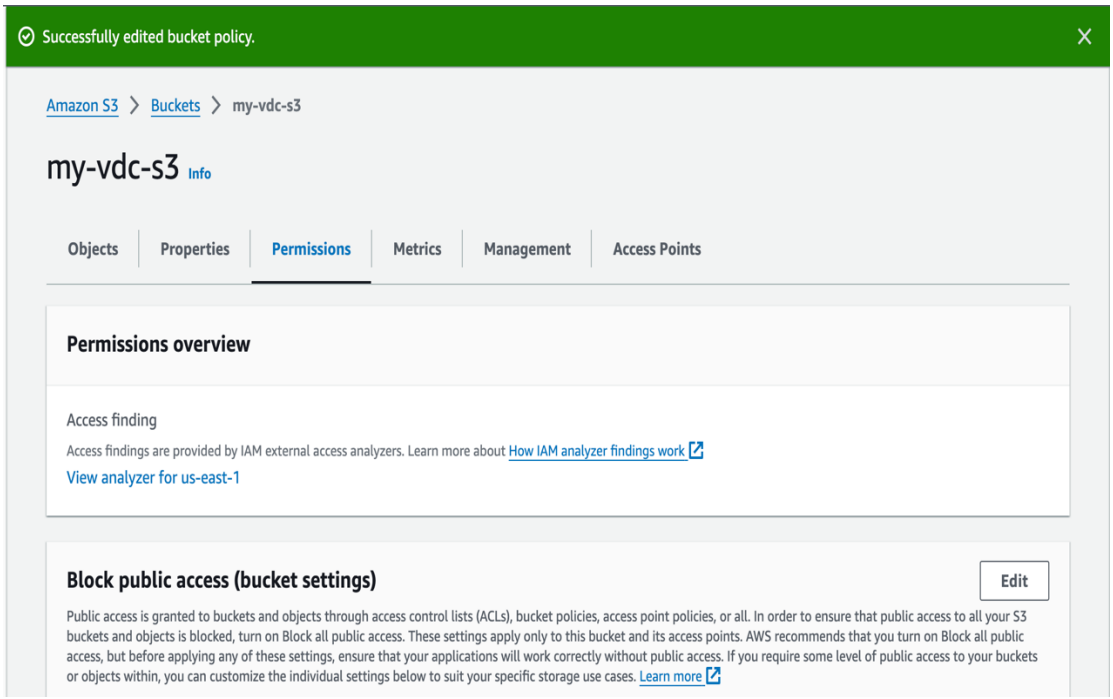


Figure 4.44. Configure S3

4.6. Detailed Instructions for Deploying DynamoDB

Open the DynamoDb console in AWS management console and click on "Create table" as shown in Figure 4.45.

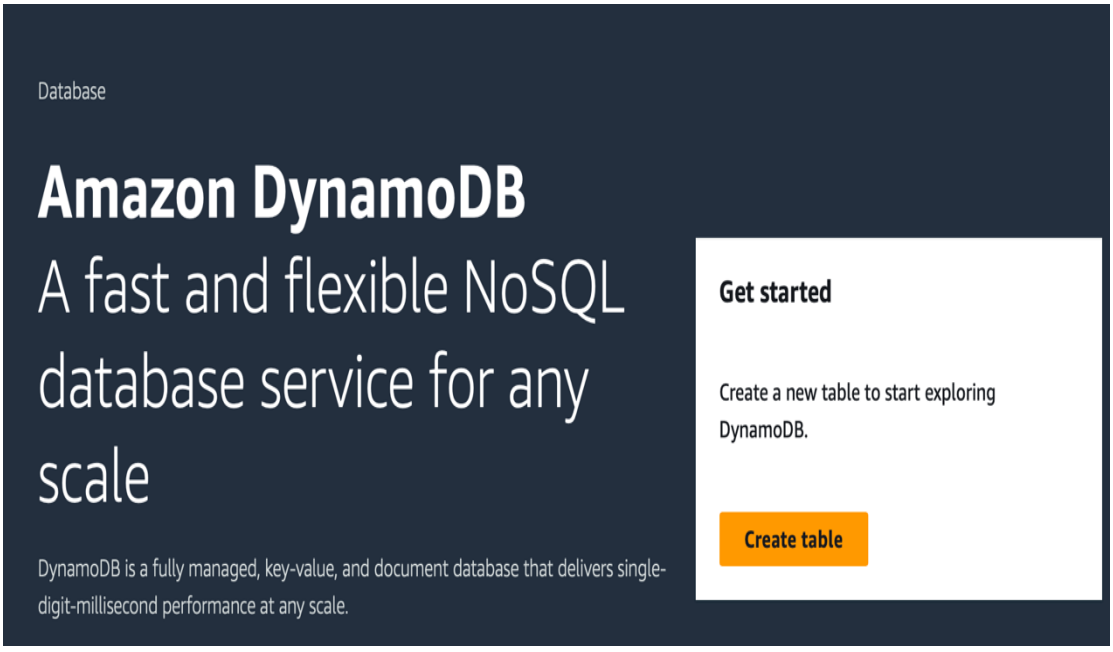


Figure 4.45. Deploy DynamoDB

As presented in Figure 4.46 enter table name and partition key .

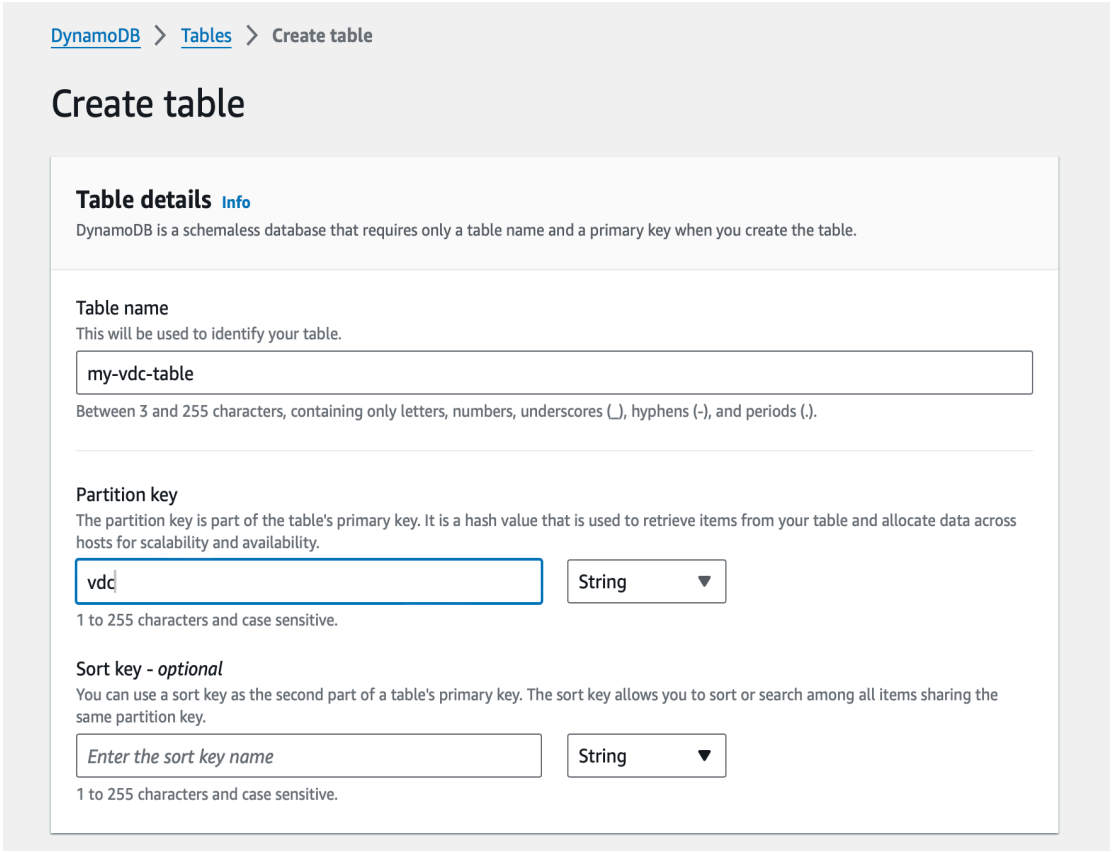


Figure 4.46. Deploy DynamoDB

Click on “Create table” button as demostrated in Figure 4.47.

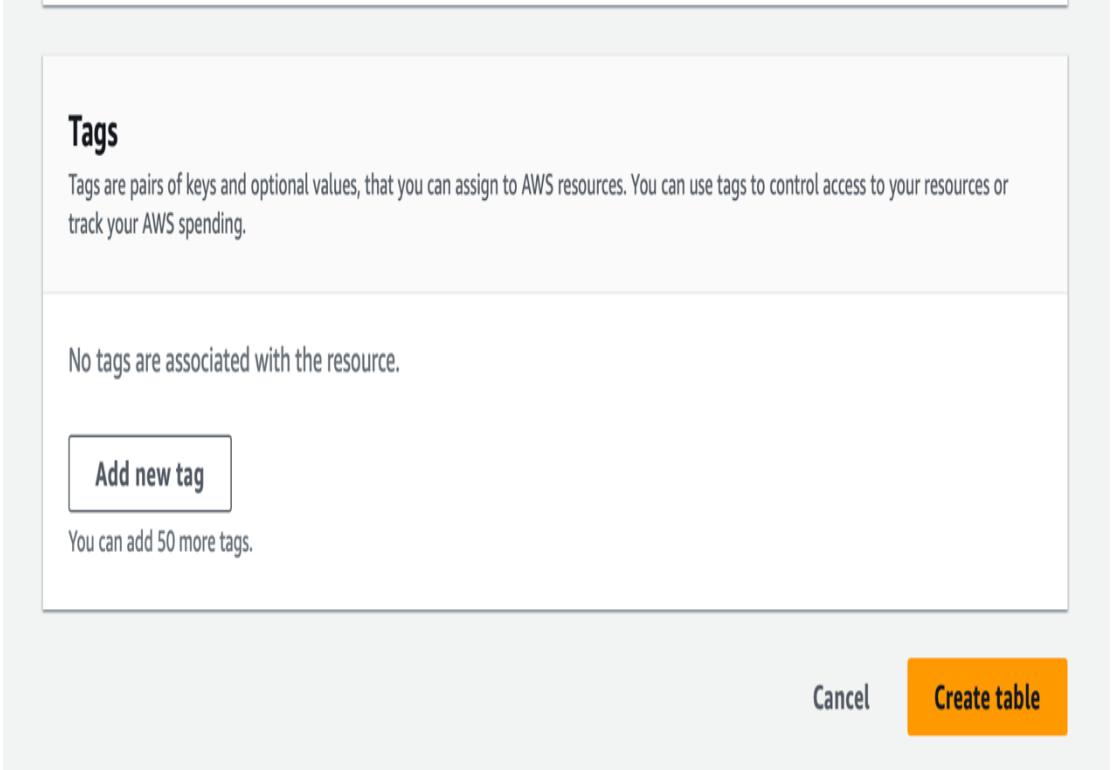


Figure 4.47. Deploy DynamoDB

4.7. Create Role for EC2 to Access S3 and DynamoDB

To create role for EC2 go access amazon S3 and DynamoDB go to IAM console, click on “Roles” in the left-hand menu and click on “Create role” as presented in Figure 4.48.

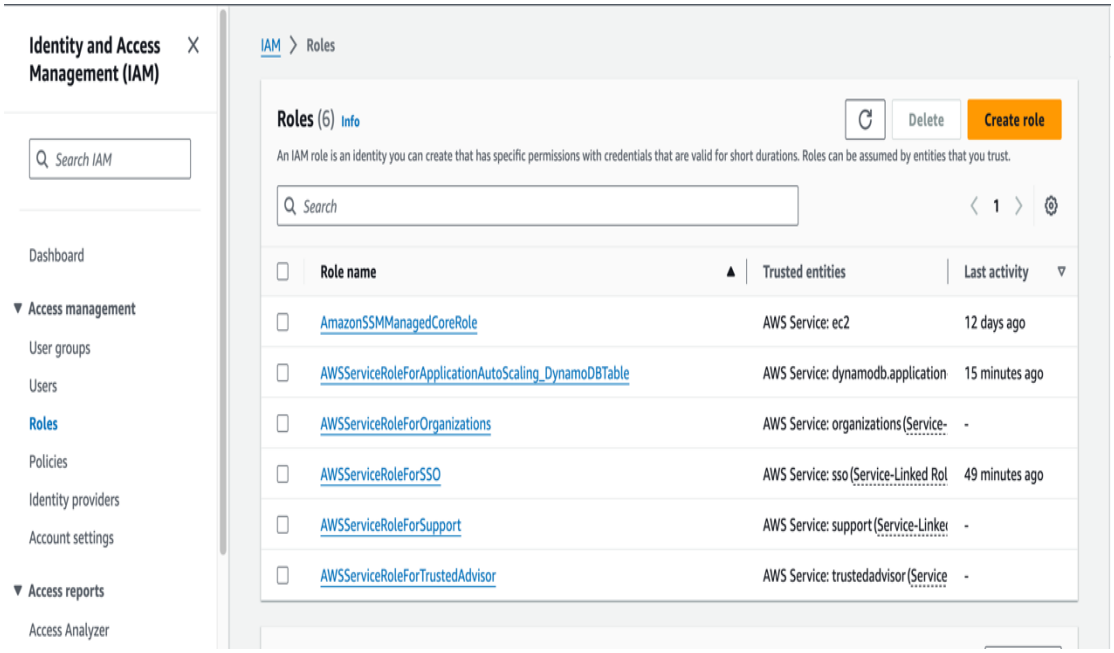


Figure 4.48. Create Role for EC2 to Access S3 and DynamoDB

Choose AWS service in tursted entity type and choose EC2 in use case as shown in Figure 4.49.

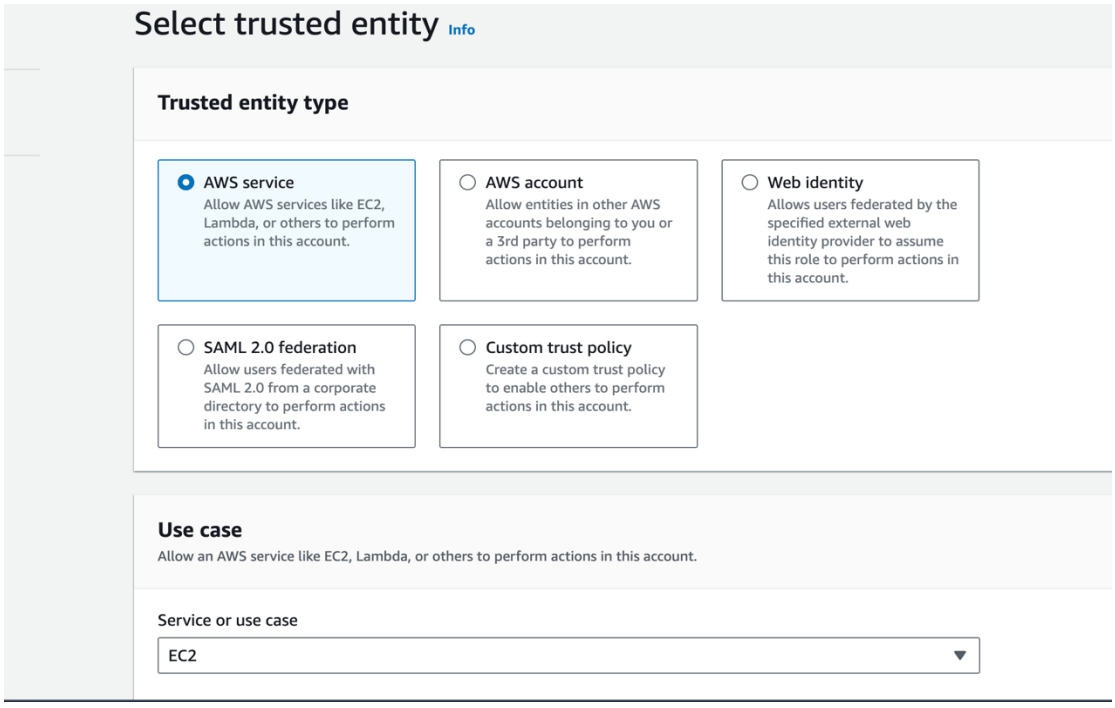


Figure 4.49. Create Role for EC2 to Access S3 and DynamoDB

As shown in Figure 4.50 enter role name and click on “Next” button.

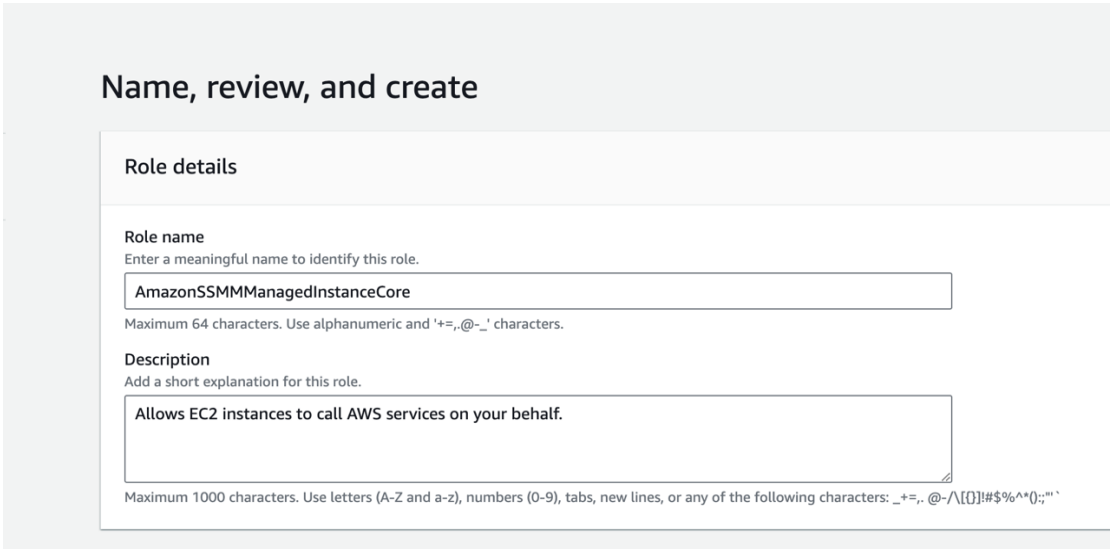


Figure 4.50. Create Role for EC2 to Access S3 and DynamoDB

Figure 4.51 presents permissions policies, attach the policies “AmazonDynamo DBFullAccess” and “AmazonS3FullAccess” to allow full access to DynamoDB and S3.

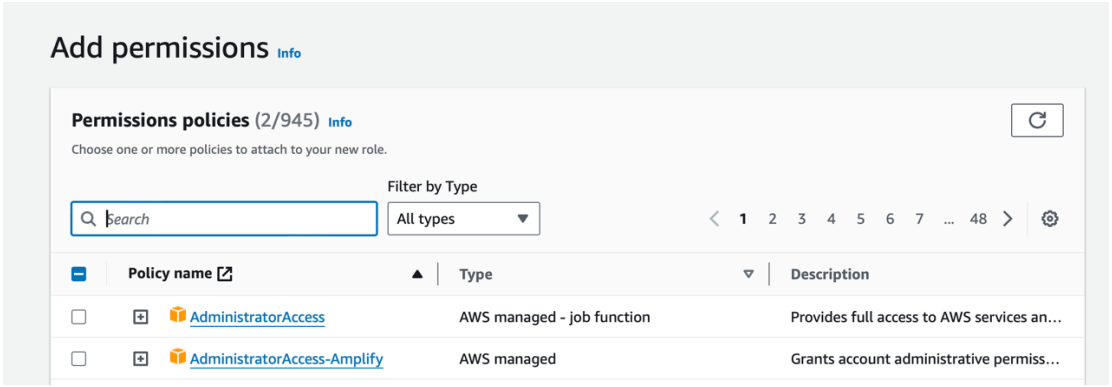


Figure 4.51. Create Role for EC2 to Access S3 and DynamoDB

Click on “Create role” as shown in Figure 4.52.

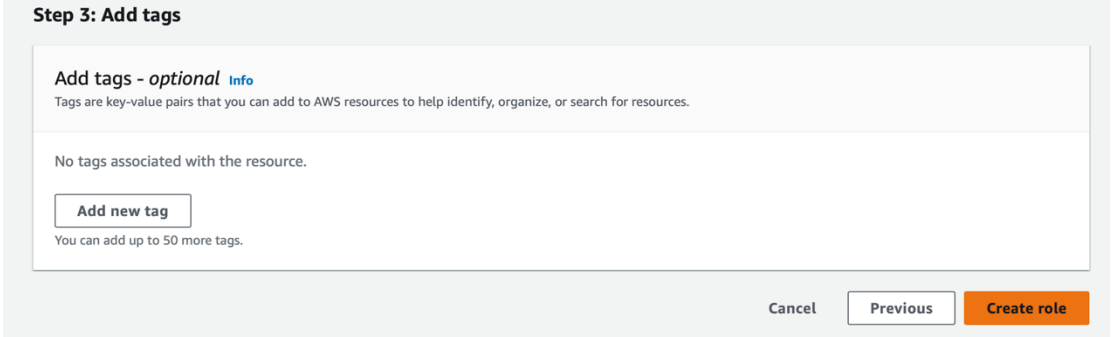


Figure 4.52. Create Role for EC2 to Access S3 and DynamoDB

4.8. Step-By-Step Guide to Create Virtual Private Network (VPC) and Set Up Network Configuration

Navigate and click VPC on AWS management console as shown in Figure 4.53.

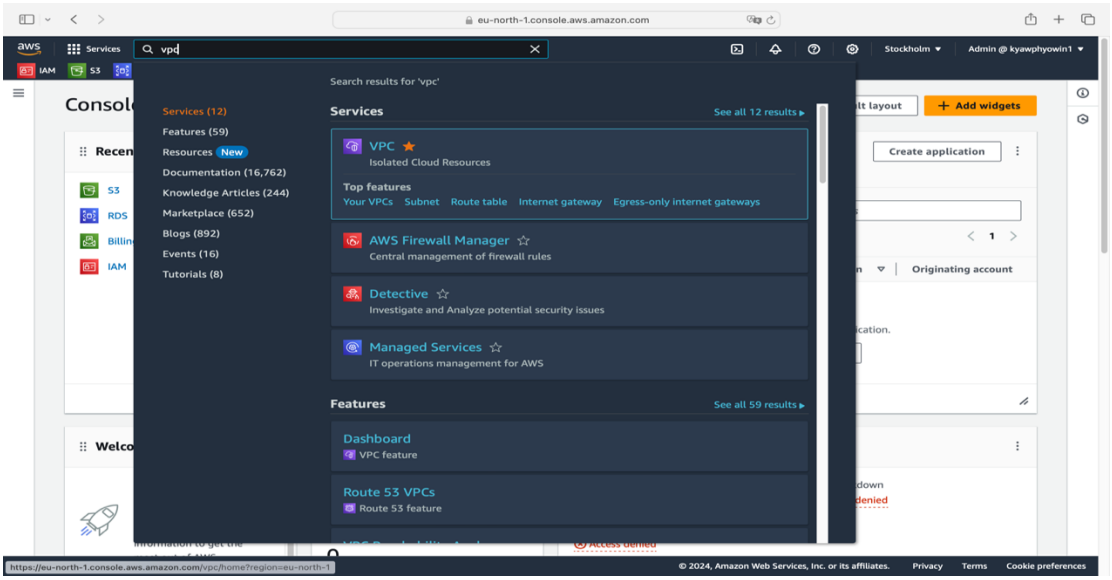


Figure 4.53. Creating VPC

As presented in Figure 4.54 click on “Create VPC”.

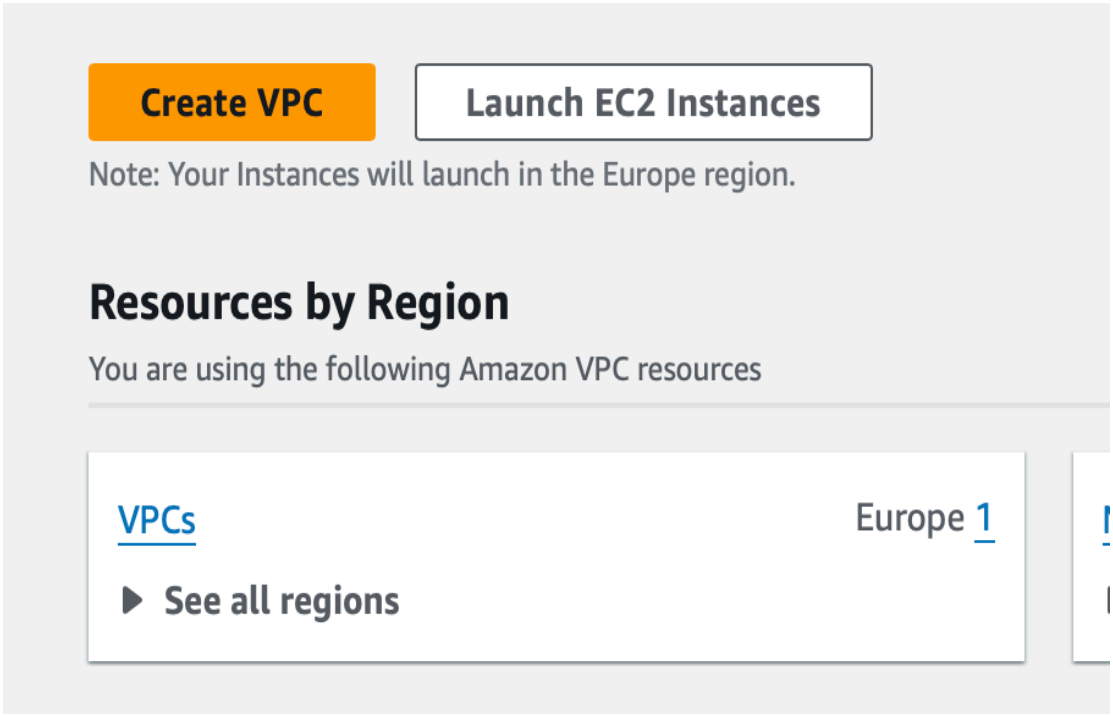


Figure 4.54. Creating VPC

As demonstrated in Figure 4.55 choose “VPC only”, enter VPC name, IPv4 CIDR block and click on “Create VPC”.

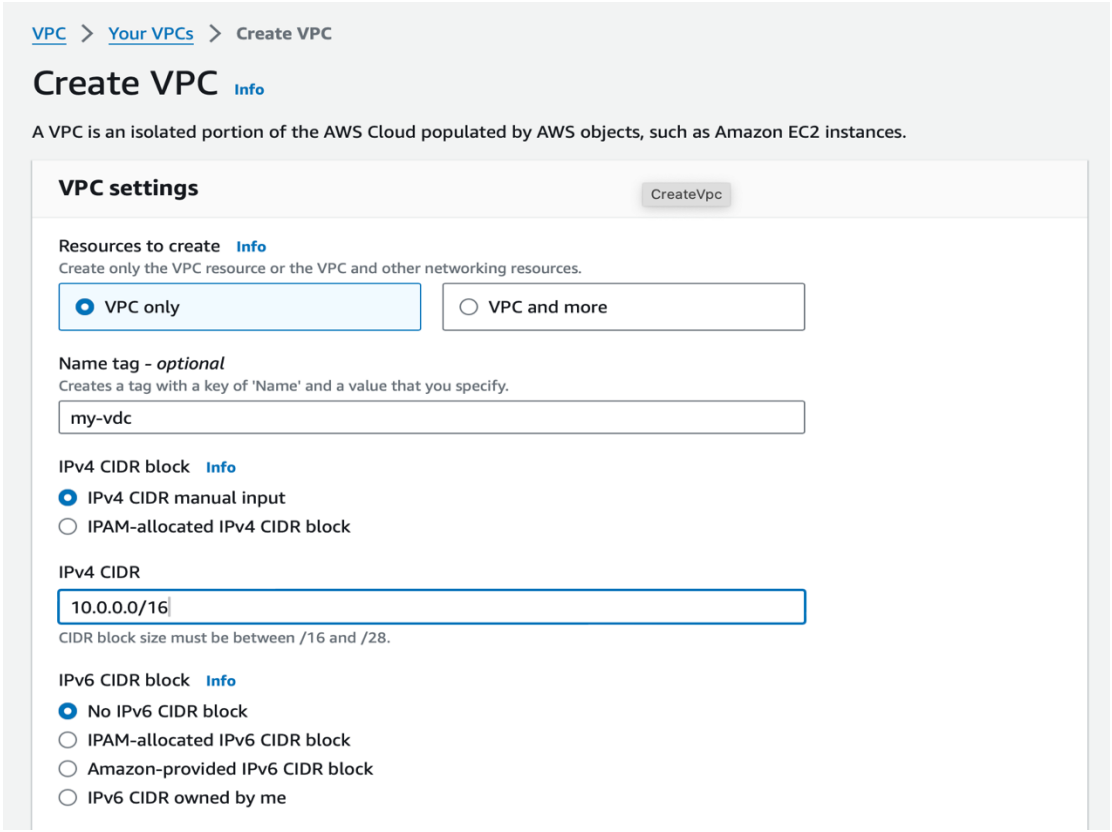


Figure 4.55. Creating VPC

Figure 4.56 presented that VPC had created successfully.

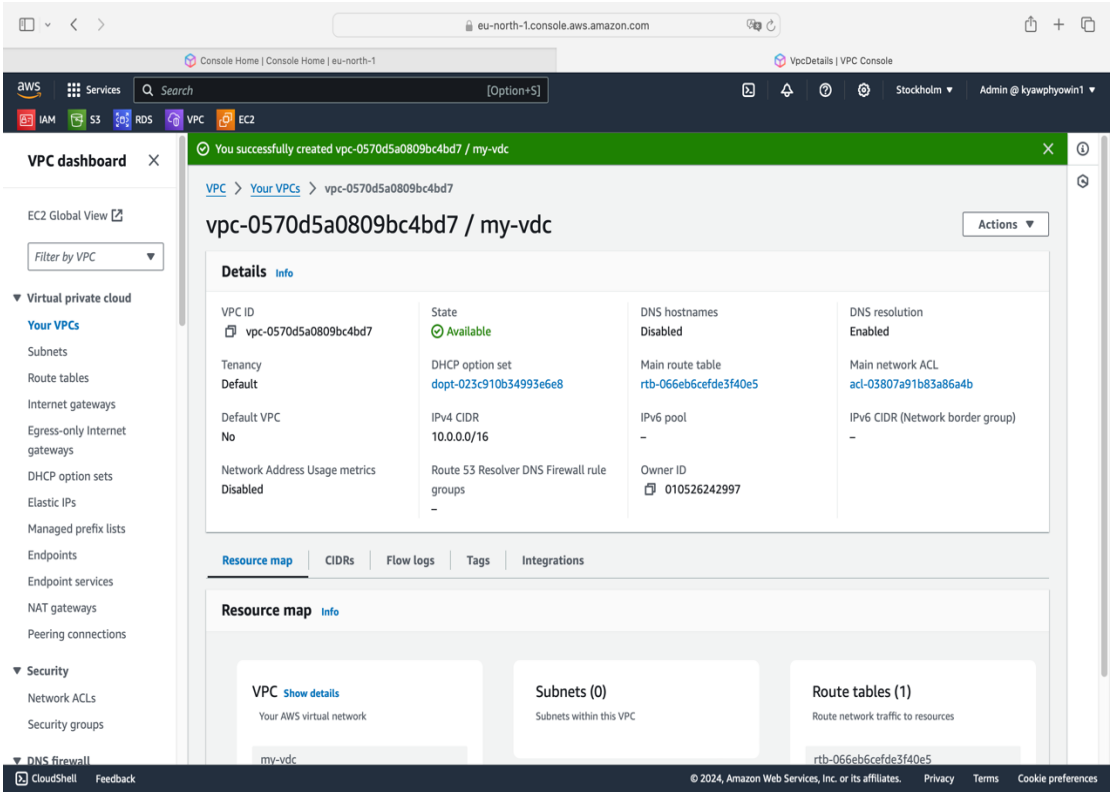


Figure 4.56. Creating VPC

Go to “Subnets” in the left-hand menu of the VPC console and click “Create Subnet” as shown in Figure 4.57.

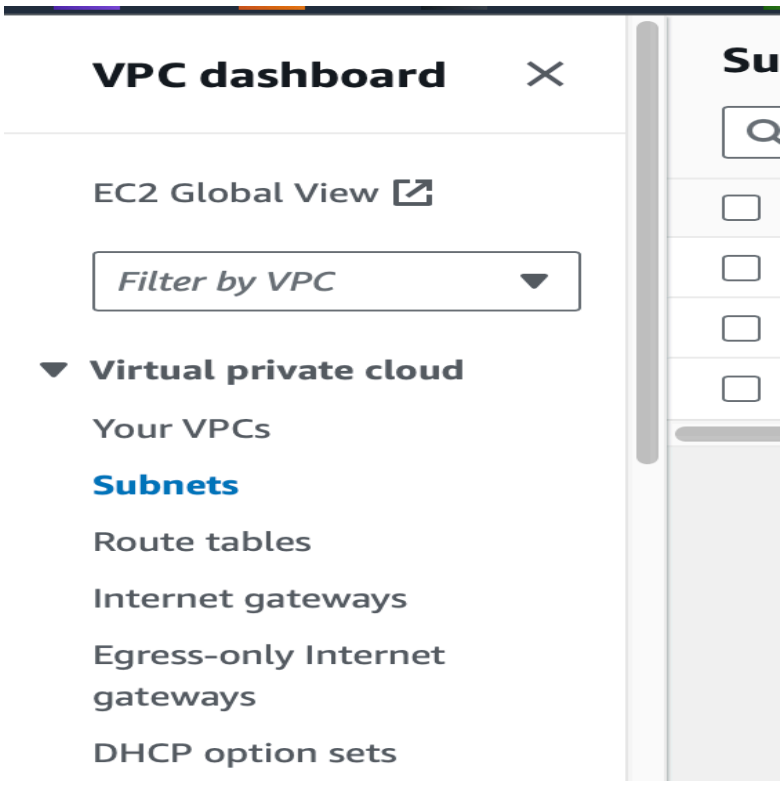


Figure 4.57. Set Up Network Configuration

As presented in Figure 4.58 choose the VPC and name the subnet.

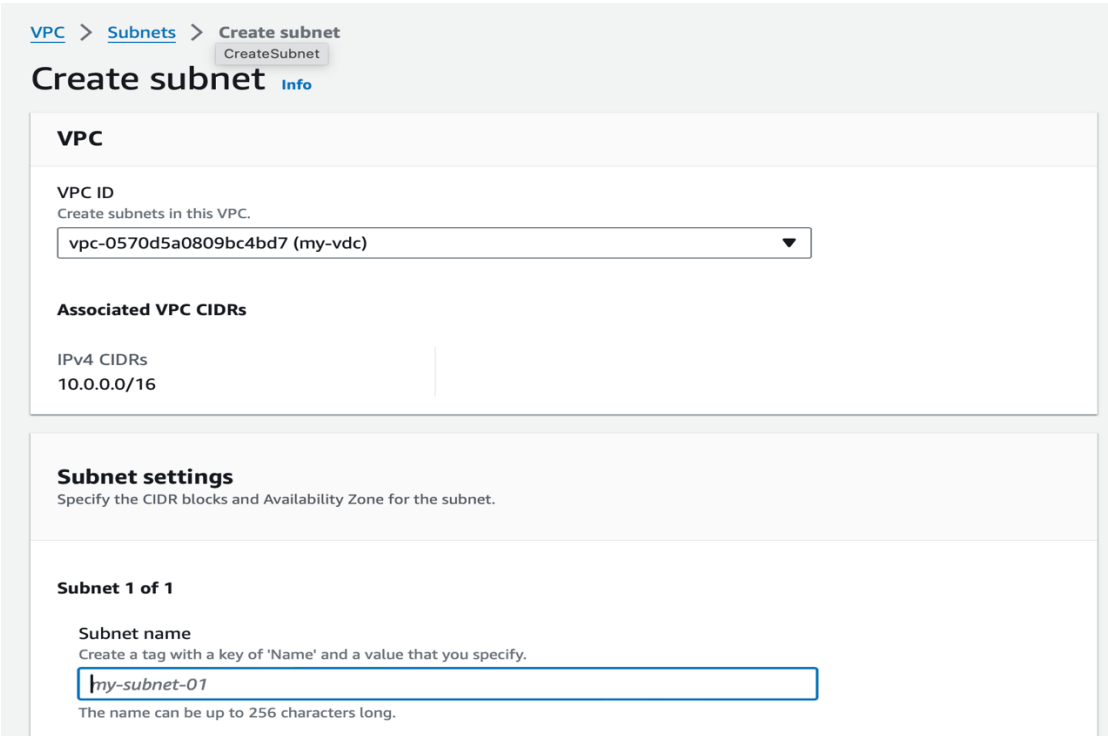


Figure 4.58. Set Up Network Configuration

As demonstrated in Figure 4.59 select CIDR block (must be within the VPC range), specify the availability zone and click “Create subnet” button.

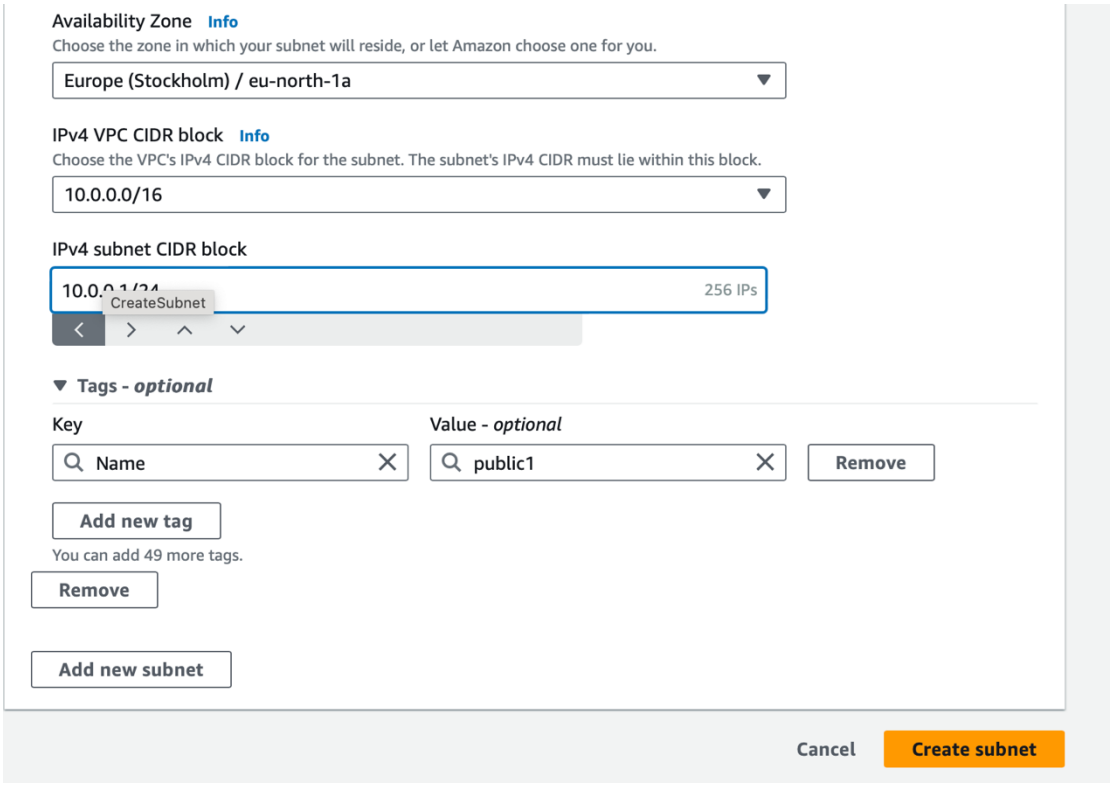


Figure 4.59. Set Up Network Configuration

As shown in Figure 4.60 check the subnet you just created, click “Actions” button at the top-right of the screen and go to “Edit subnet settings”.

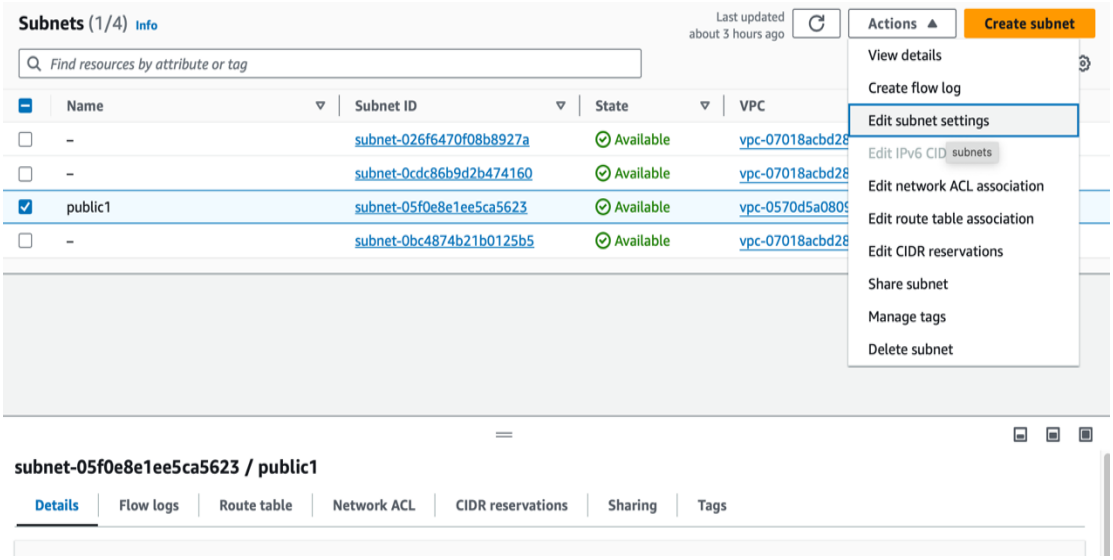


Figure 4.60. Set Up Network Configuration

Check “Enable auto-assign public IPv4 address” as presented in Figure 4.61.

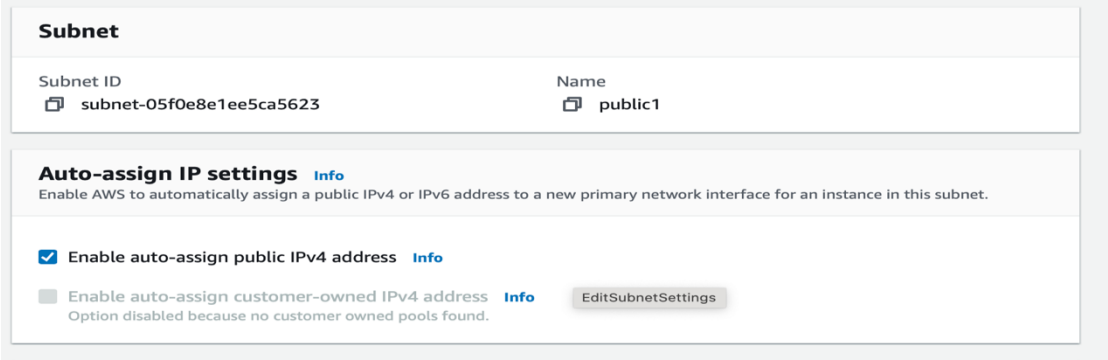


Figure 4.61. Set Up Network Configuration

In the VPC console left menu, go to Internet Gateways" and click "Create Internet Gateway as demonstrated in Figure 4.62.

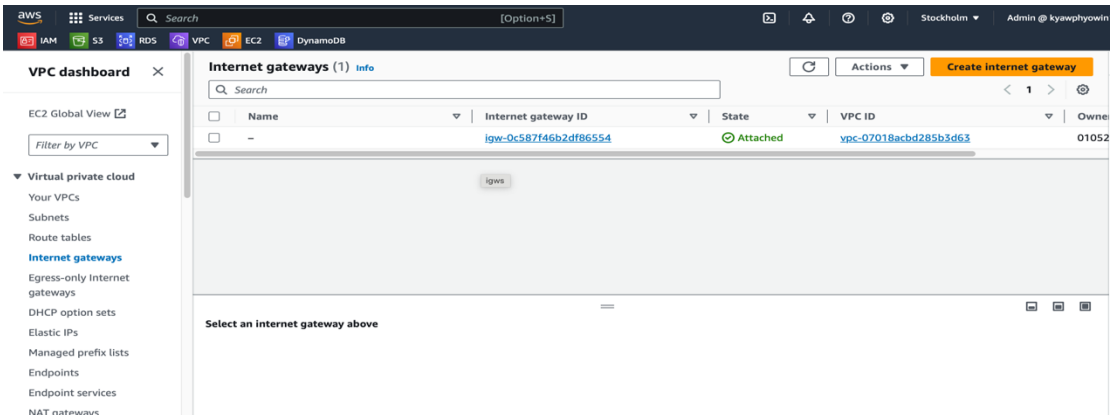


Figure 4.62. Set Up Network Configuration

Name the internet gateway and click "Create internet gateway" button as shown in Figure 4.63.

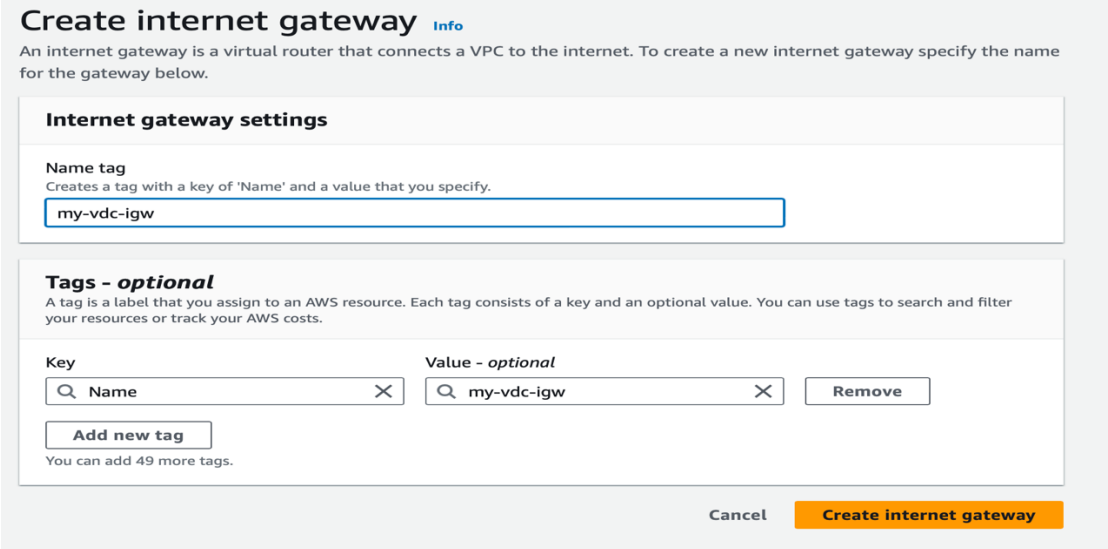


Figure 4.63. Set Up Network Configuration

Click on “Actions” button on the top-right of the screen and go to “Attach to VPC” as shown in Figure 4.64.

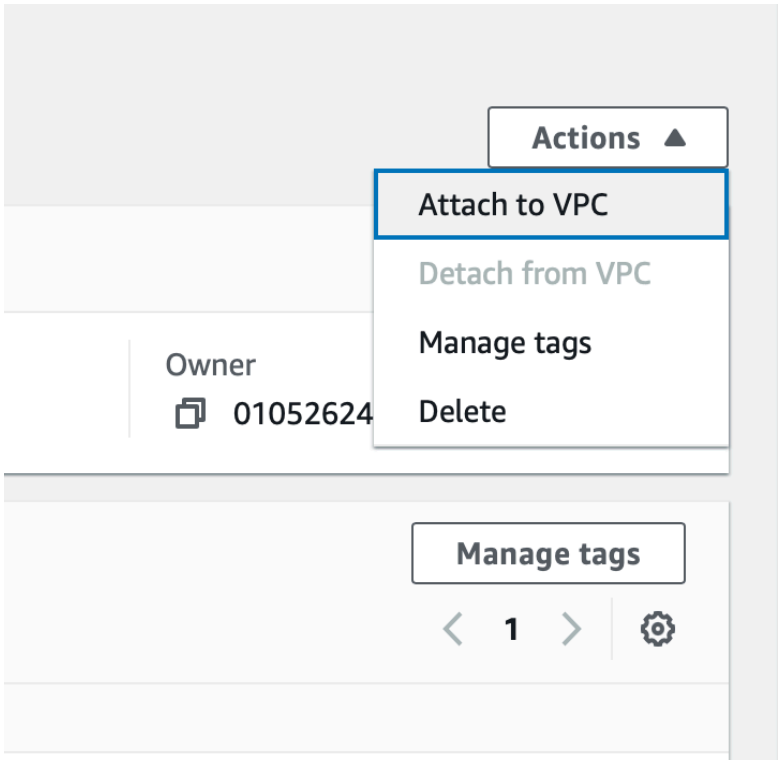


Figure 4.64. Set Up Network Configuration

As shown in Figure 4.65 choose the VPC and click “Attach internet gateway”. Internet gateway creation was completed successfully.

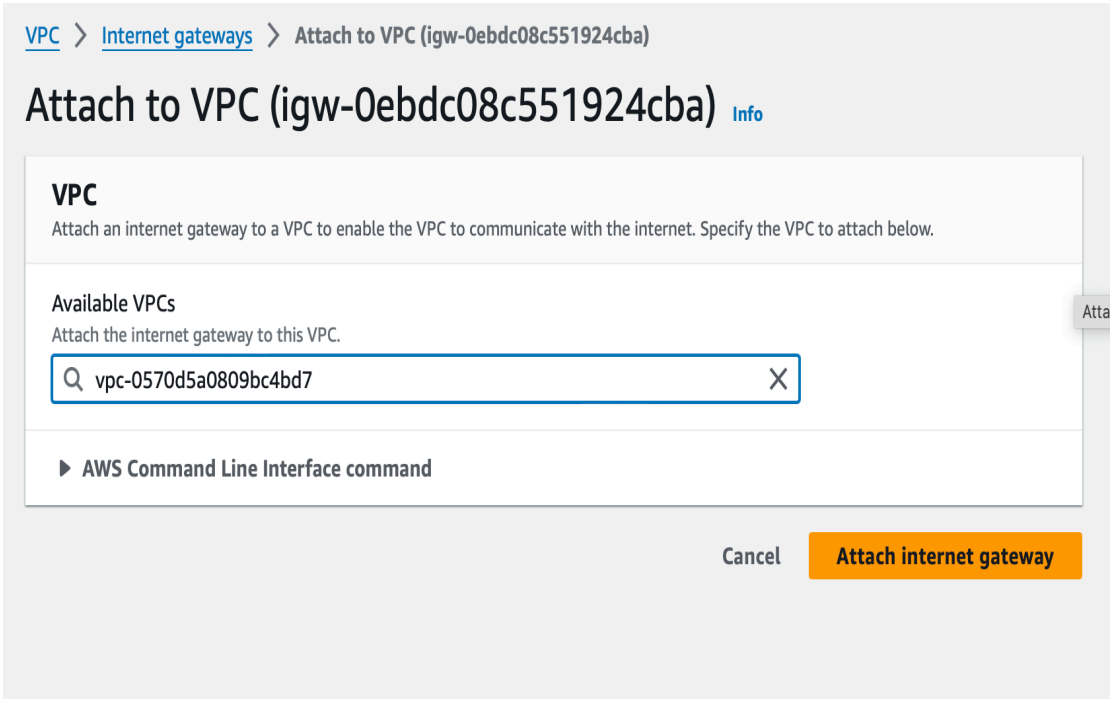


Figure 4.65. Set Up Network Configuration

In the VPC console, go to “Route Tables” and click “Create route table” as presented in Figure 4.66. And name the route table, select VPC and click on “Create” button.

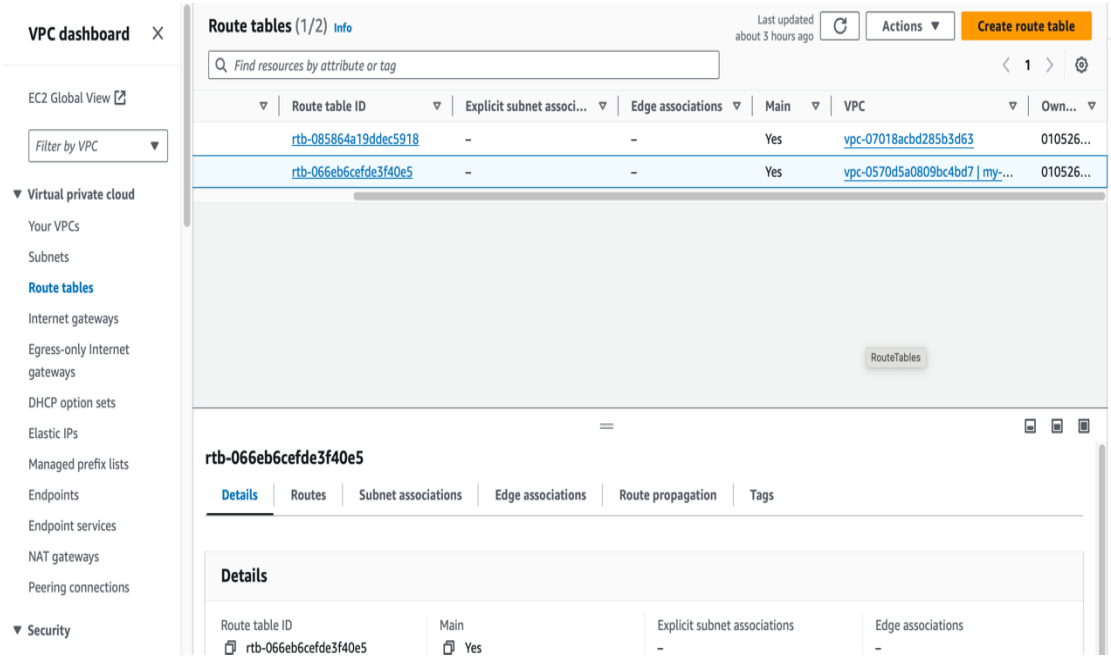


Figure 4.66. Set Up Network Configuration

As demonstrated in Figure 4.67 select the route table and click “Edit routes”.

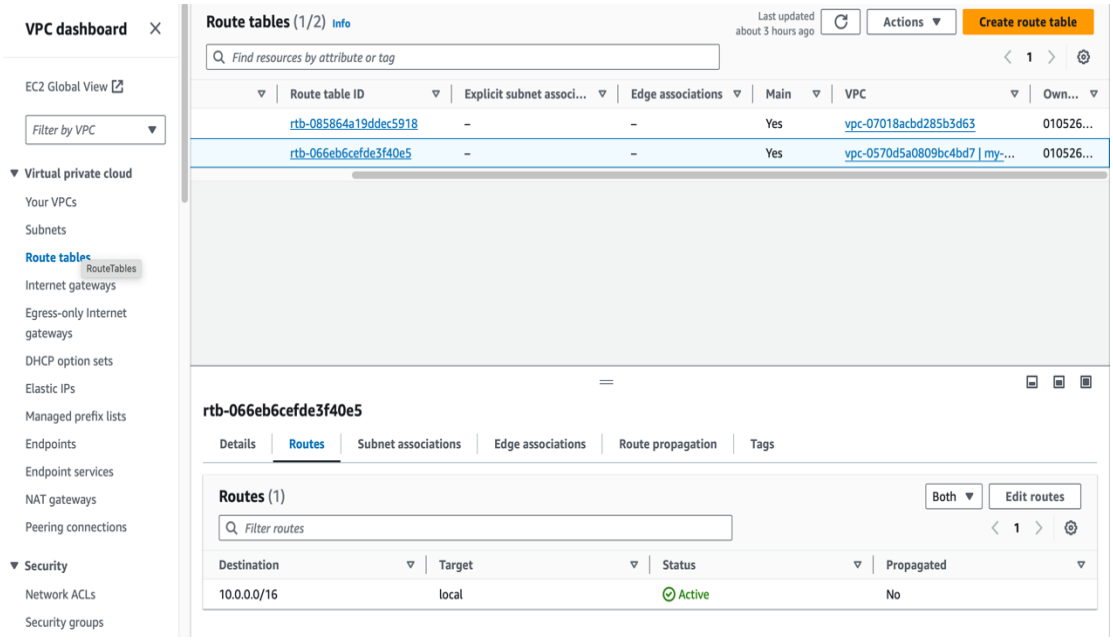


Figure 4.67. Set Up Network Configuration

Click “Add route” and select “0.0.0.0/0” in destination and add your internet gateway on target and click “Save route” as shown in Figure 4.68.

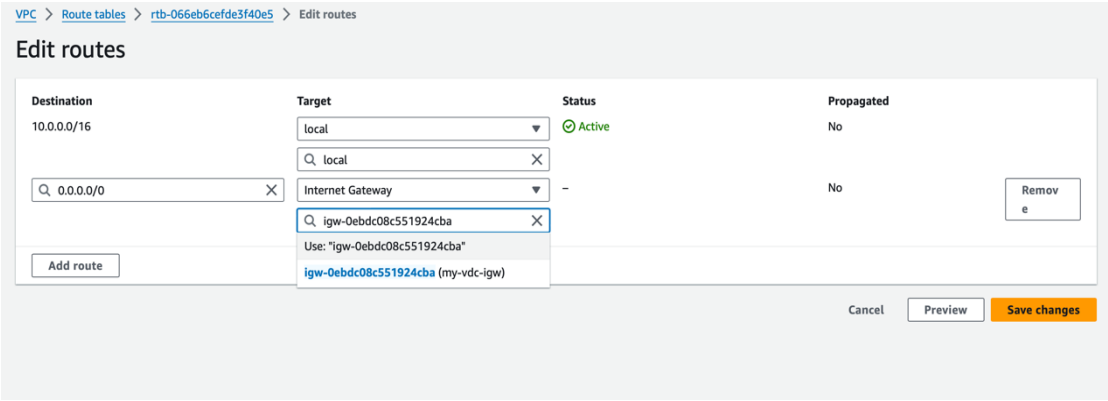


Figure 4.68. Set Up Network Configuration

As presented in Figure 4.69 select “Subnet associations” tab and click “Edit subnet associations”.

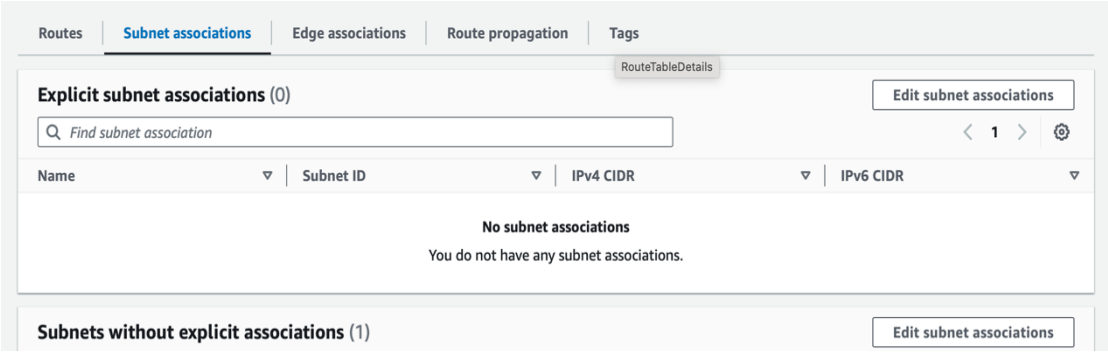


Figure 4.69. Set Up Network Configuration

Select your public subnet and click “Save associations” as demonstrated in Figure 4.70.

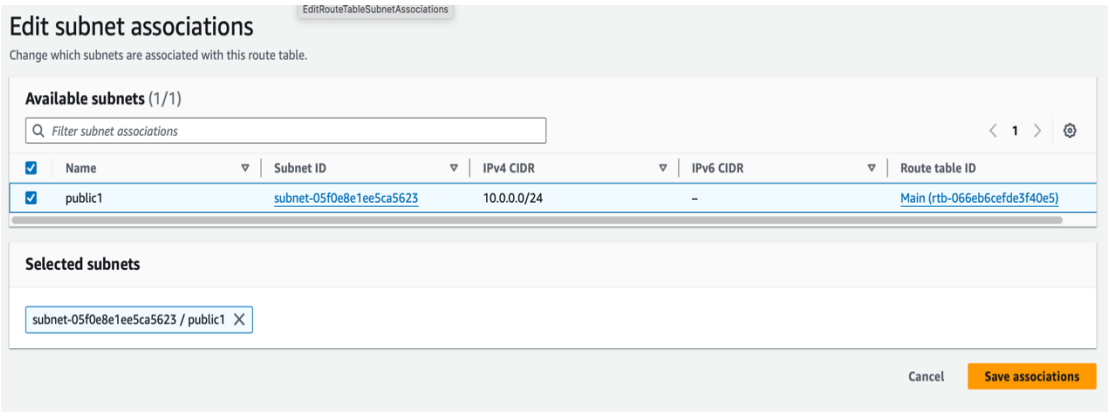


Figure 4.70. Set Up Network Configuration

Go to “Security groups” on the left menu and click on “Create security group” as presented in Figure 4.71.

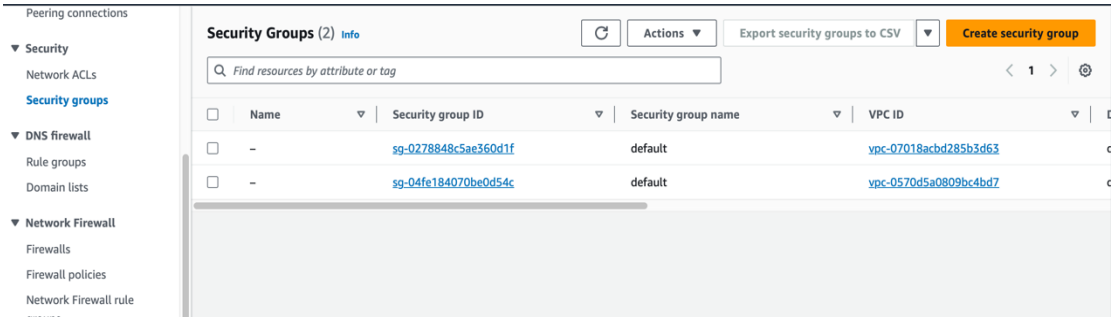


Figure 4.71. Set Up Network Configuration

As demonstrated in Figure 4.72 name the security group, add description and select VPC.

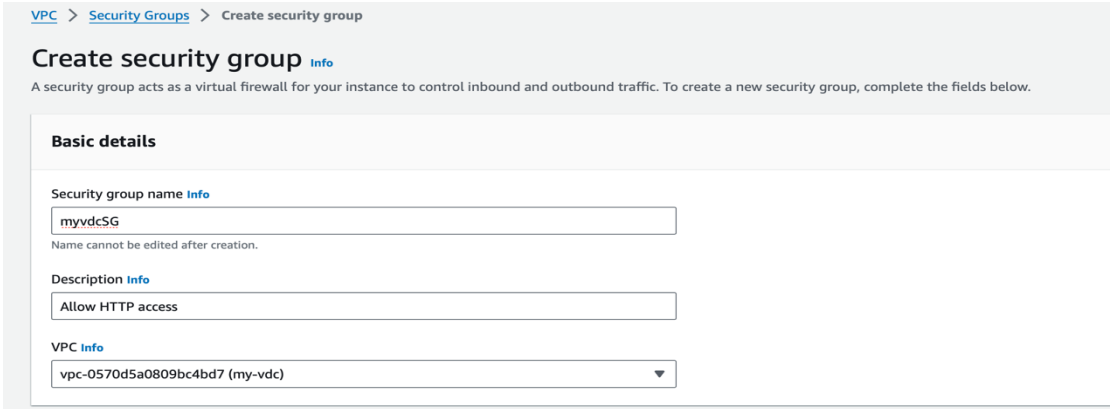


Figure 4.72. Set Up Network Configuration

Click on “Add rule”, select the type of traffic “HTTP”, define where the traffic is allowed from (e.g. 0.0.0.0/0) and click on “Create security group” as shown in Figure 4.73.

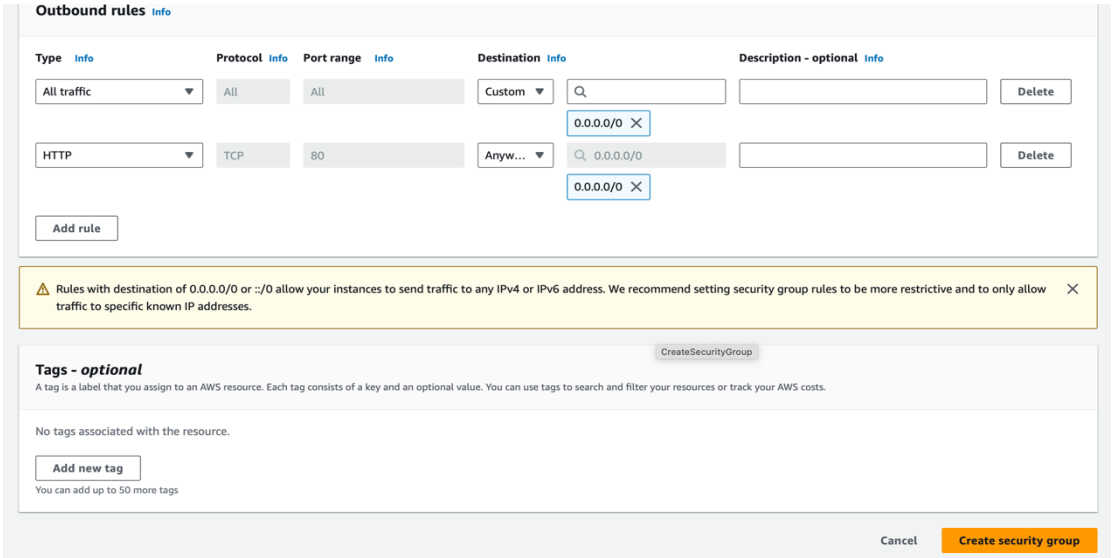
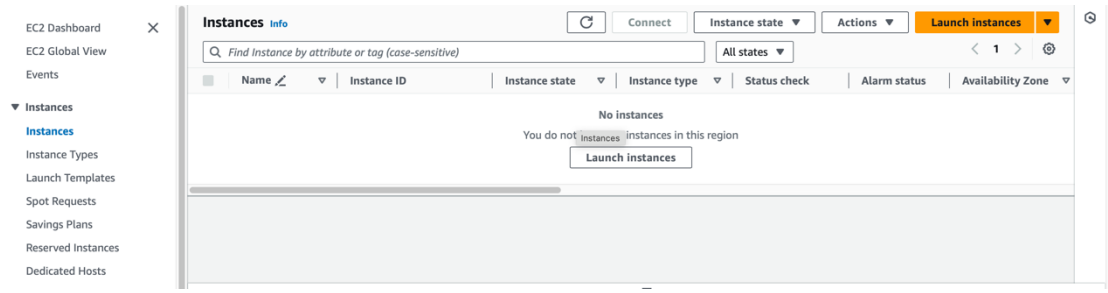


Figure 4.73. Set Up Network Configuration

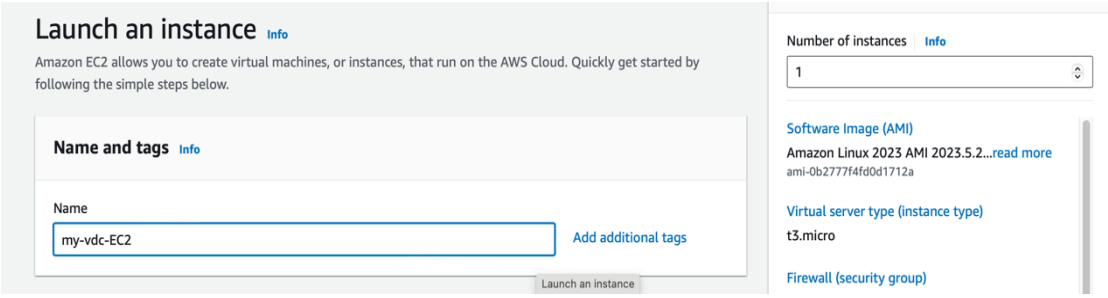
4.9. Step-By-Step Guide to Launch Elastic Compute Cloud (EC2)

Navigate to EC2 under the “Compute” section, click on “Launch Instance” as shown in Figure 4.74.



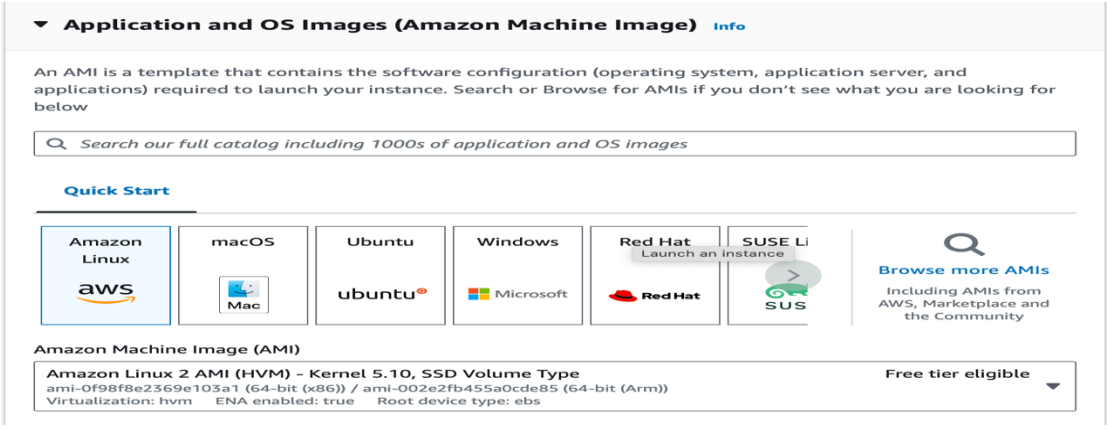
4.74. Launch EC2 Instance

As presented in Figure 4.75 name the instance.



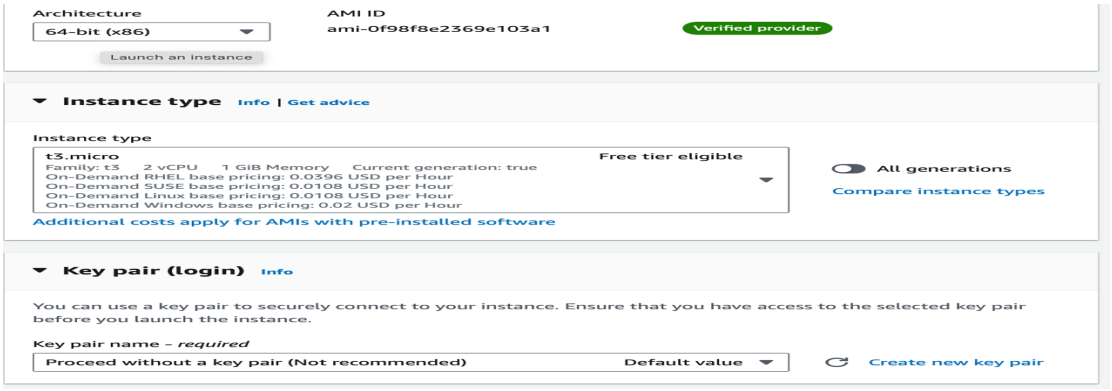
4.75. Launch EC2 Instance

Figure 4.76 shows Amazon Machine Image(AMI), select the AMI that best fits your needs.



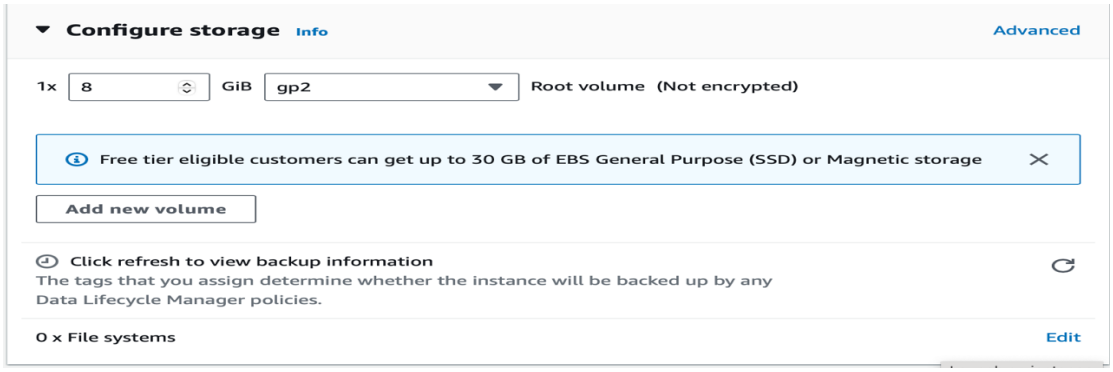
4.76. Launch EC2 Instance

Figure 4.77 presents the instance types, select an instance type based on the required CPU, memory, network performance and create keypair for remote connection to EC2.



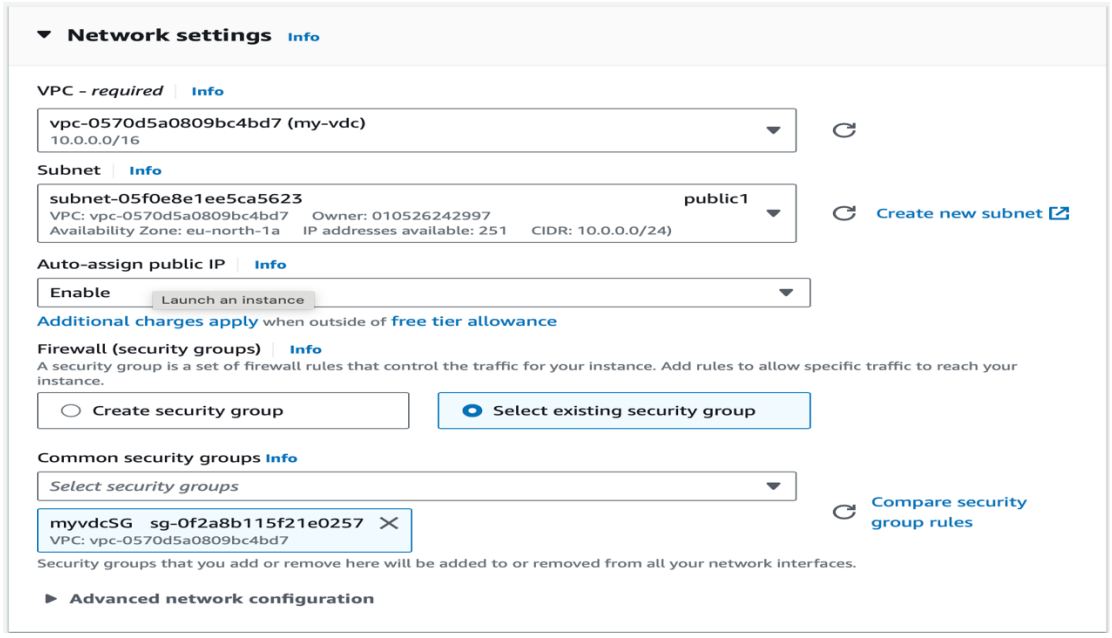
4.77. Launch EC2 Instance

As demonstrated in Figure 4.78 configure storge as your needs.



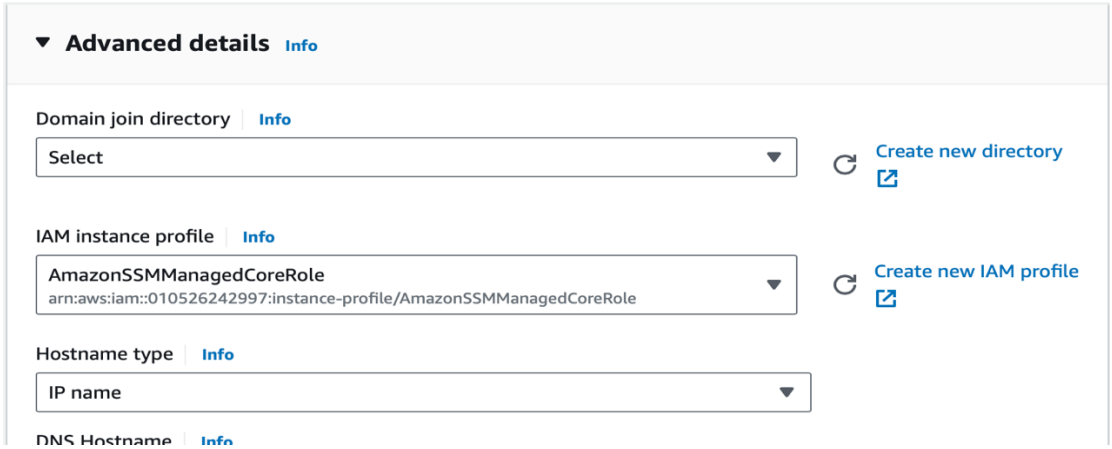
4.78. Launch EC2 Instance

Figure 4.79 demonstrates network setting, choose VPC and public subnet, ensure “Auto-assign public IP” is enable for public access and select security group.



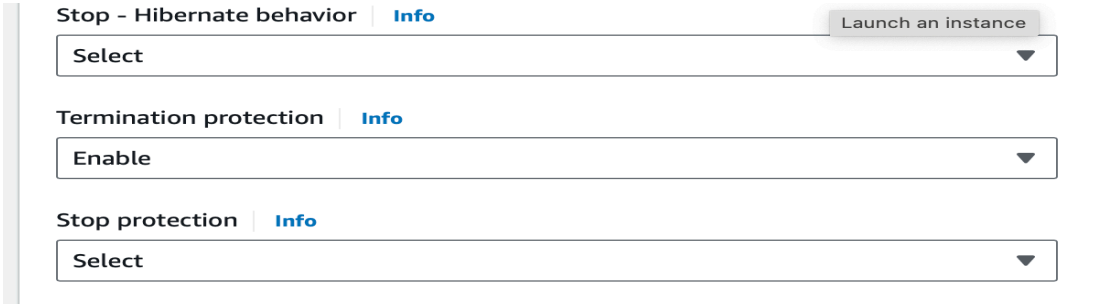
4.79. Launch EC2 Instance

Open “Advance details” and add “AmazonSSMManagedCoreRole” role in IAM instance profile to access S3 and DynamoDB as demonstrated in Figure 4.80.



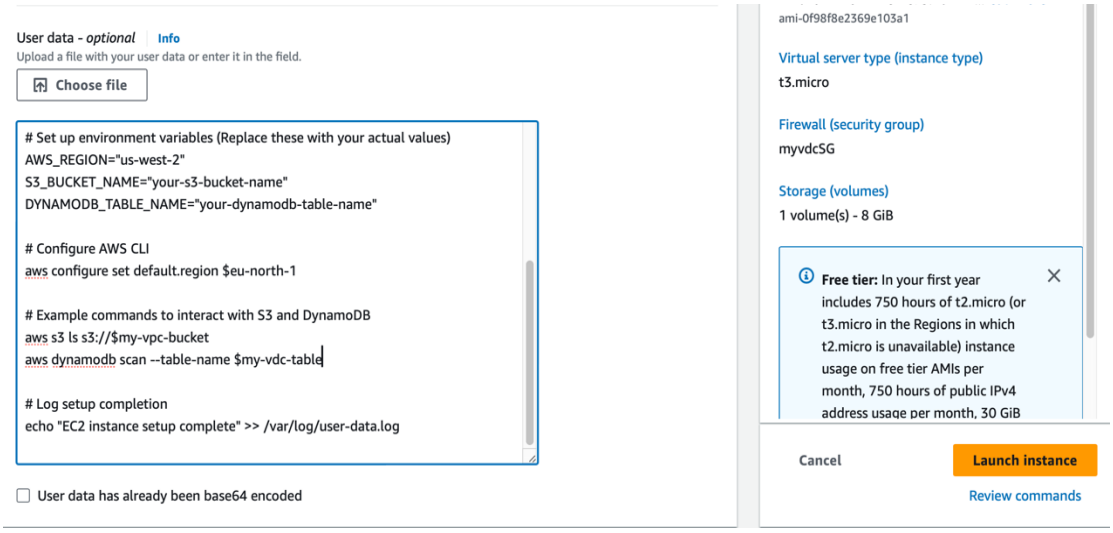
4.80. Launch EC2 Instance

Scroll down and select “Enable” on “Termination protection as shown in Figure 4.81.



4.81. Launch EC2 Instance

And then scroll down and click on “Launch instance” as shown in Figure 4.82.



4.82. Launch EC2 Instance

Wait until 2/2 checks passed on “Status check” as shown in Figure 4.83.

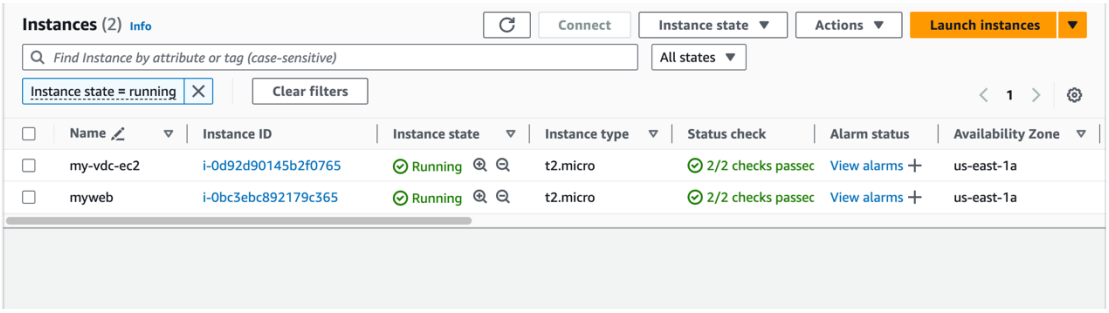


Figure 4.83. Launch EC2 Instance

4.10. Creating an Datadog account and Sign Up

Visit “datadogdh.com” and click on “Get started free” for create datadog account as shown in Figure 4.84.

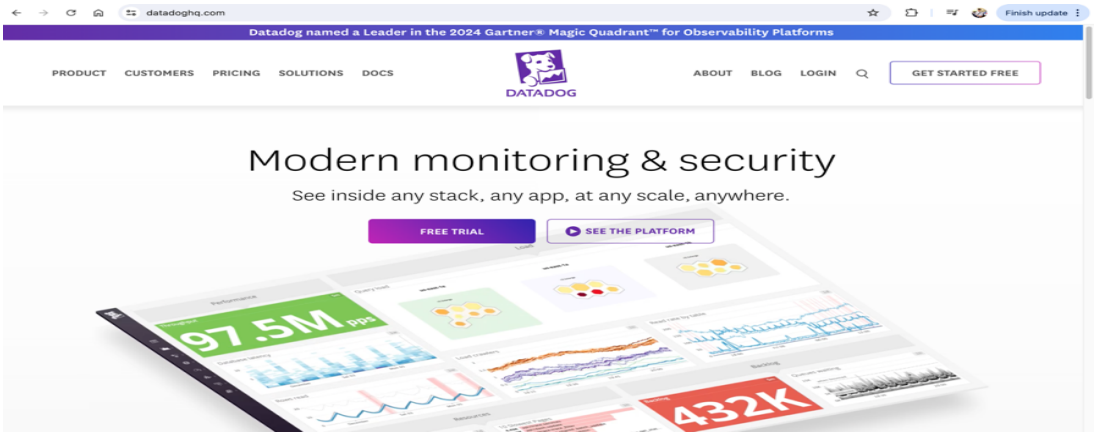


Figure 4.84. Sign Up Datadog Monitoring Framework

Fill the required information to create datadog account as presented in Figure 4.85.

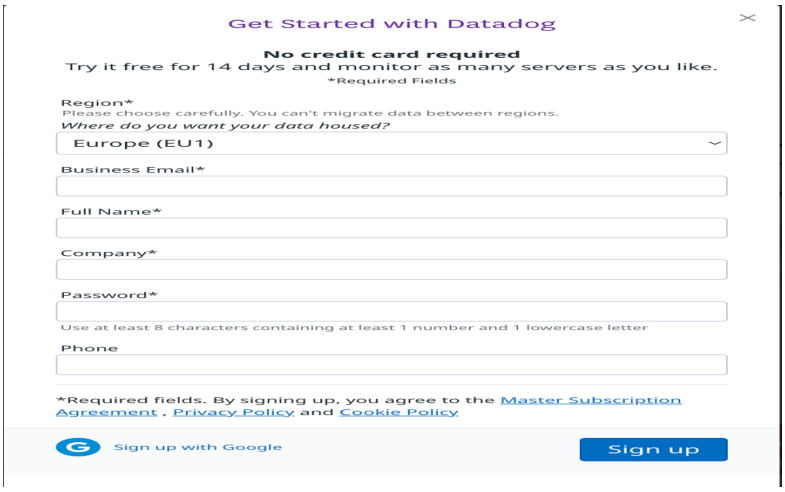


Figure 4.85. Sign Up Datadog Monitoring Framework

To confirm email enter code that sent to email as demonstrated in Figure 4.86.

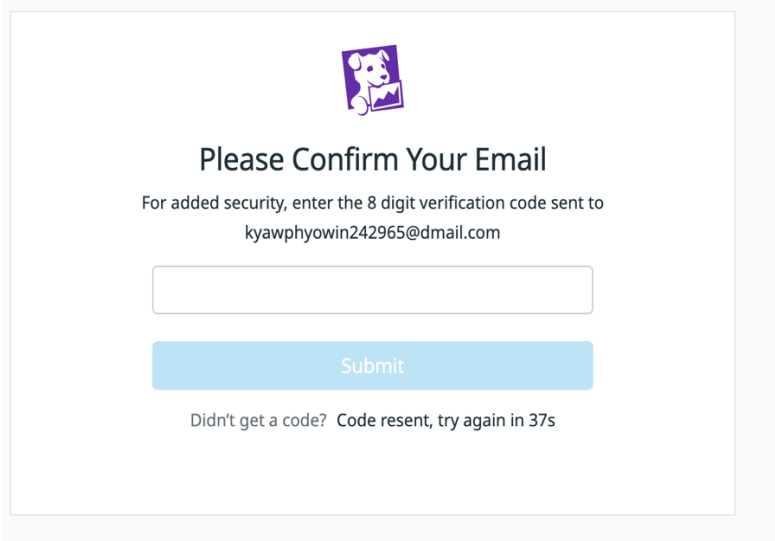


Figure 4.86. Sign Up Datadog Monitoring Framework

4.11. Integrate Datadog with AWS

Figure 4.87 presents several services and software that can integrate with datadog , choose AWS services to integrate.

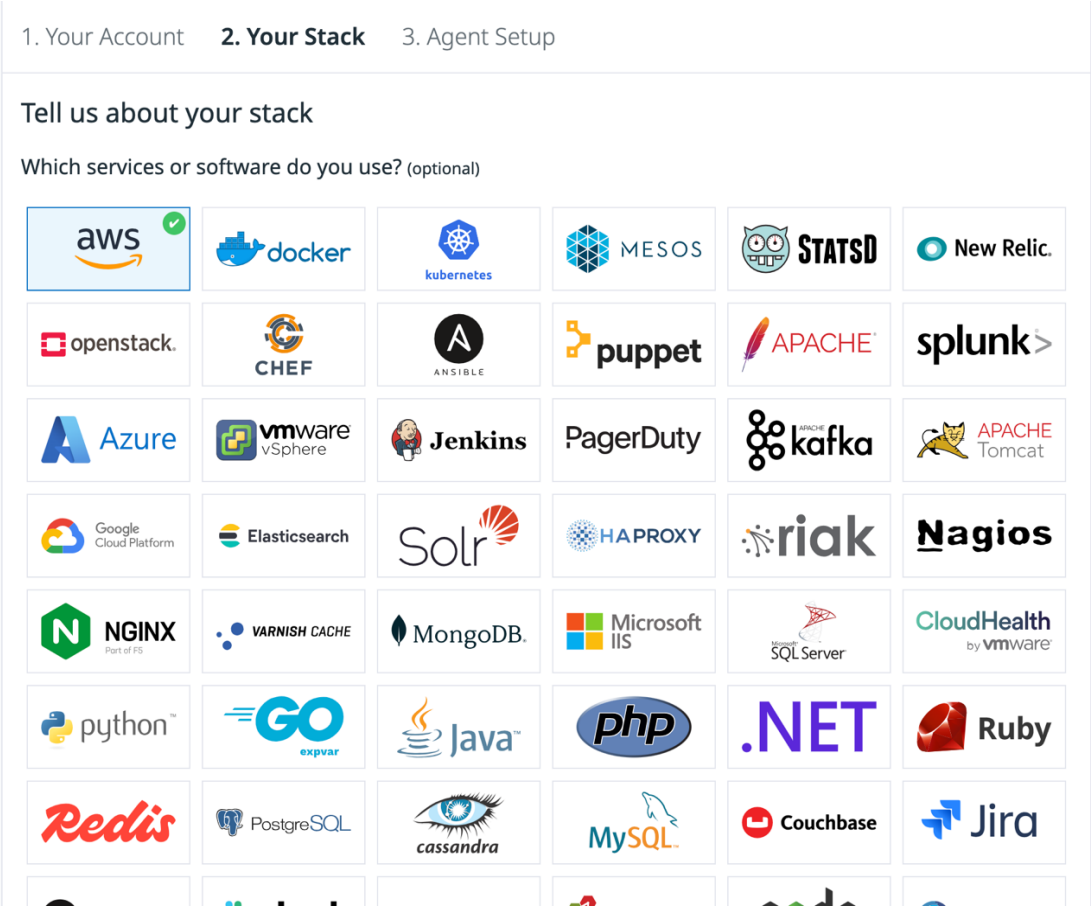


Figure 4.87. Integrate Datadog with AWS

To install the agent choose agent type as shown in Figure 4.88.

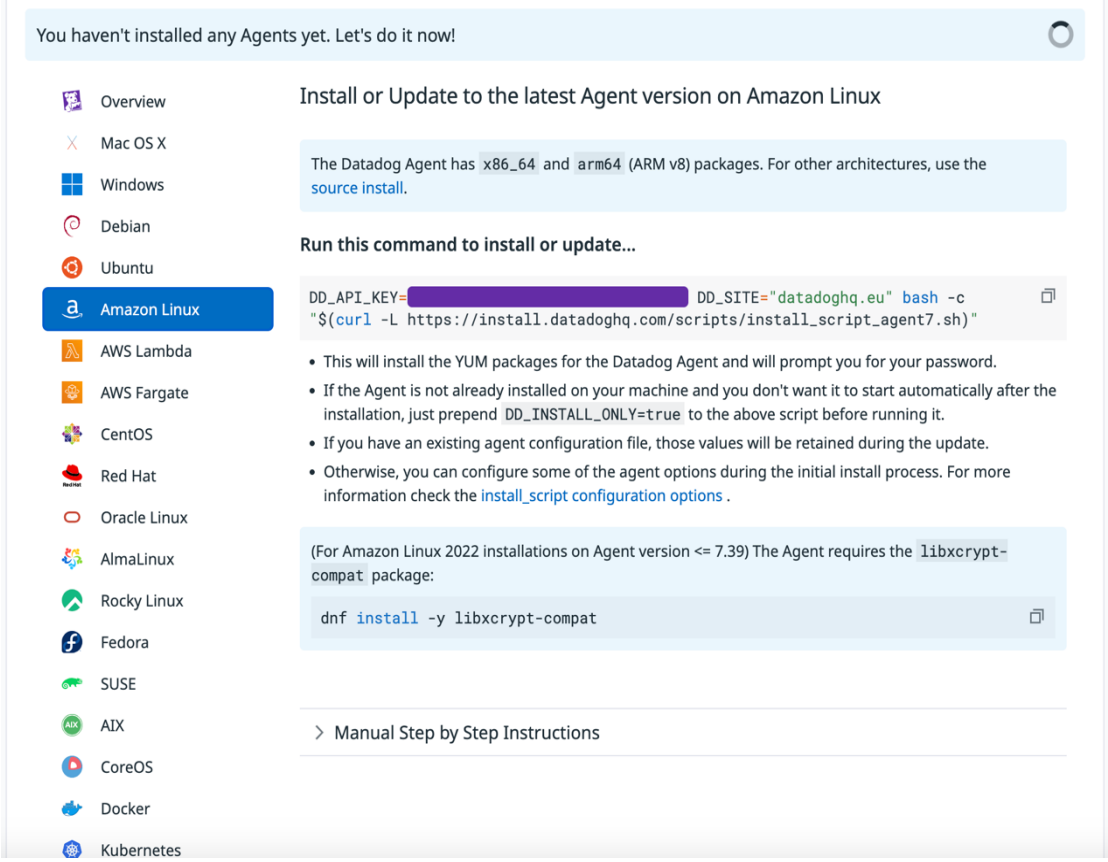


Figure 4.88. Integrate Datadog with AWS

As demonstrated in Figure 4.89 make SSH connection with EC2 with terminal and install the datadog agent with the following commands: “DD_AGENT_MAJOR _VERSION=7 DD_API_KEY=your_api_key_here DD_SITE ="datadoghq.com" bash -c "$(curl -L https://s3.amazonaws.com/dd-agent/scripts /install_script.sh)"”.

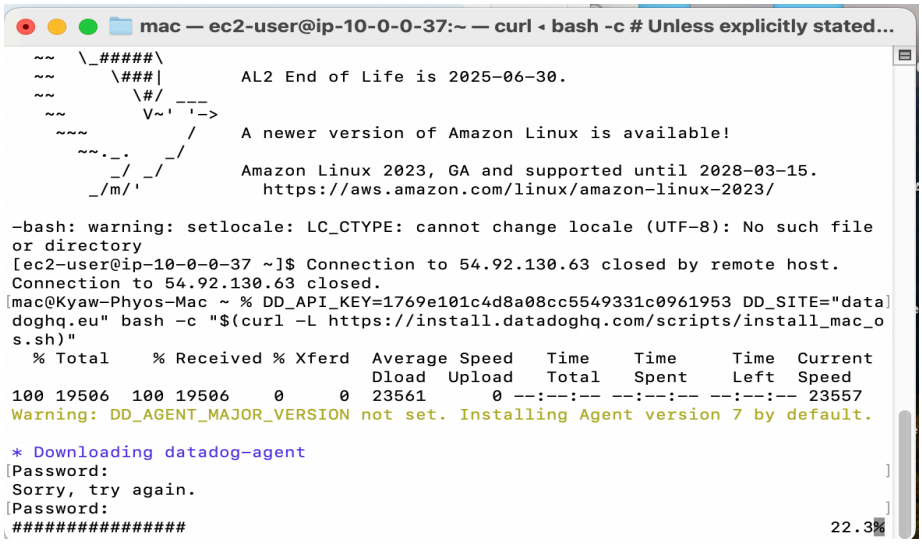


Figure 4.89. Integrate Datadog with AWS

Access the datadog home and click on “Create a Dashboard” as presented in Figure 4.90.

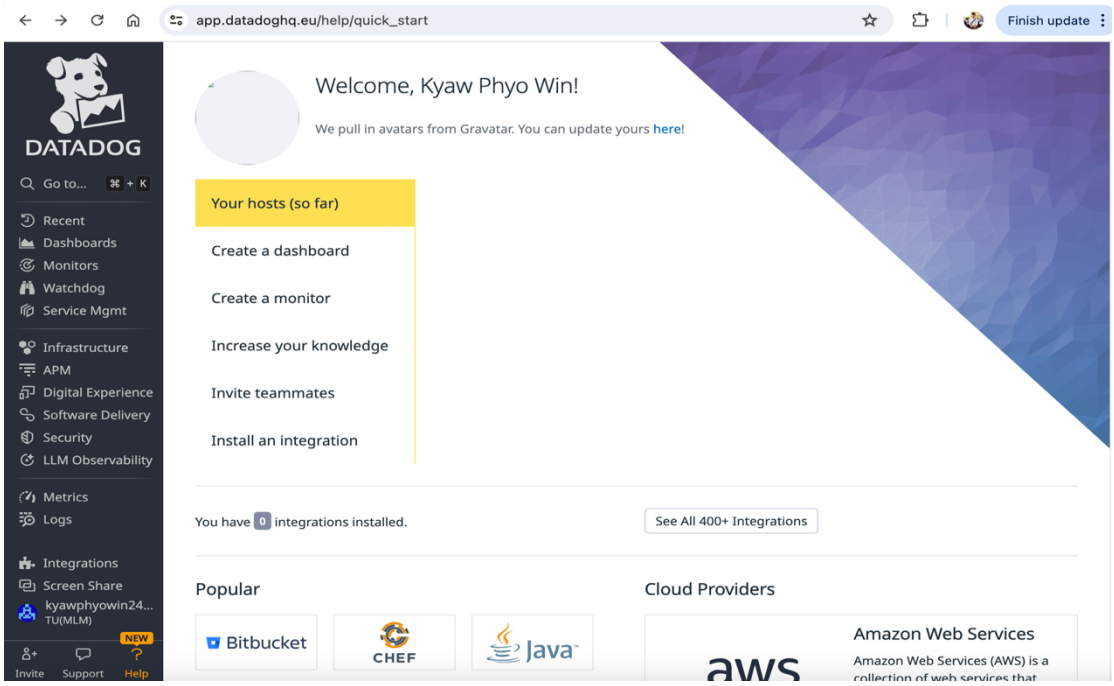


Figure 4.90. Integrate Datadog with AWS

Choose “Amazon Web Services” as shown in Figure 4.91.

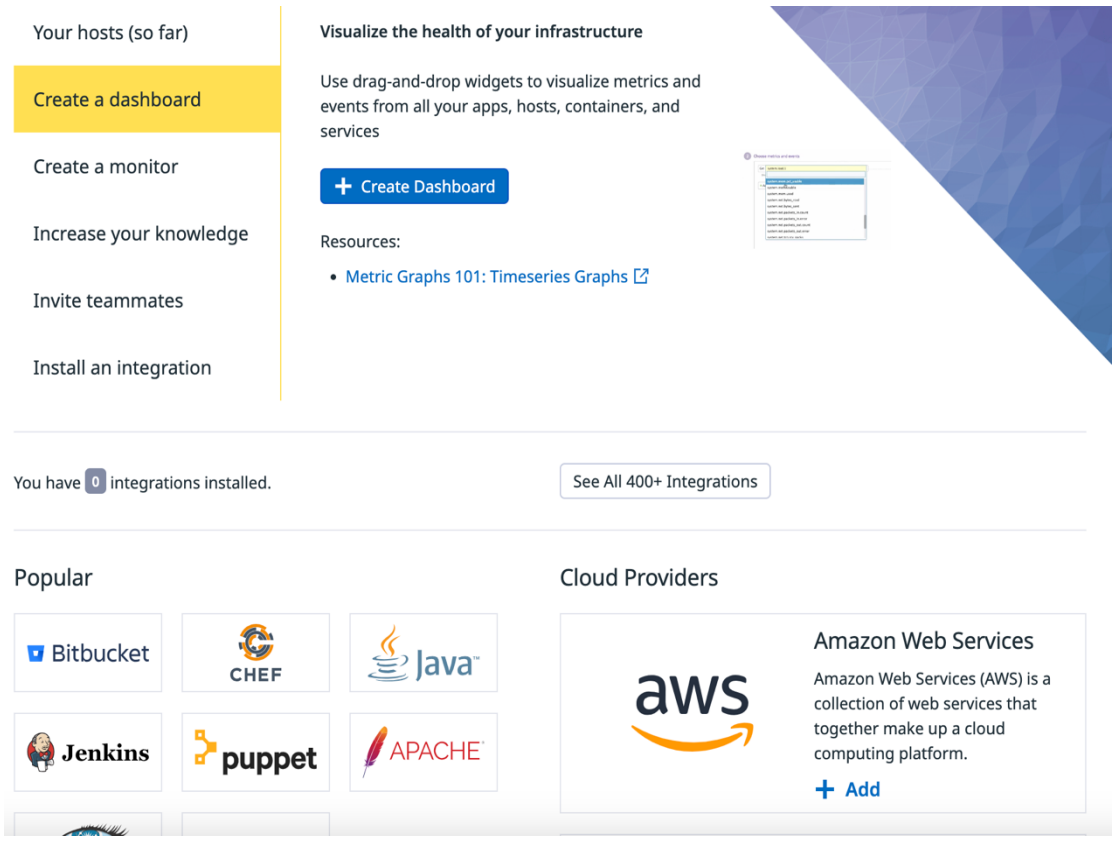


Figure 4.91. Integrate Datadog with AWS

Click on “Add AWS Account” as demonstrated in Figure 4.92.

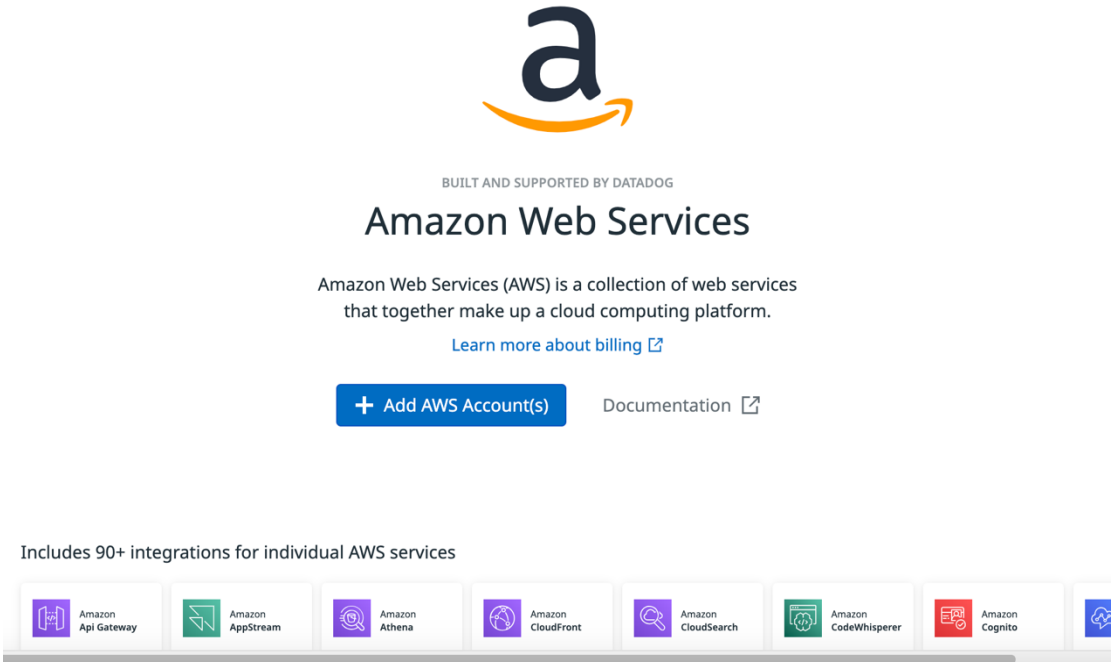


Figure 4.92. Integrate Datadog with AWS

Choose a method for adding AWS account and click on “View Documentation” as presented in Figure 4.93.

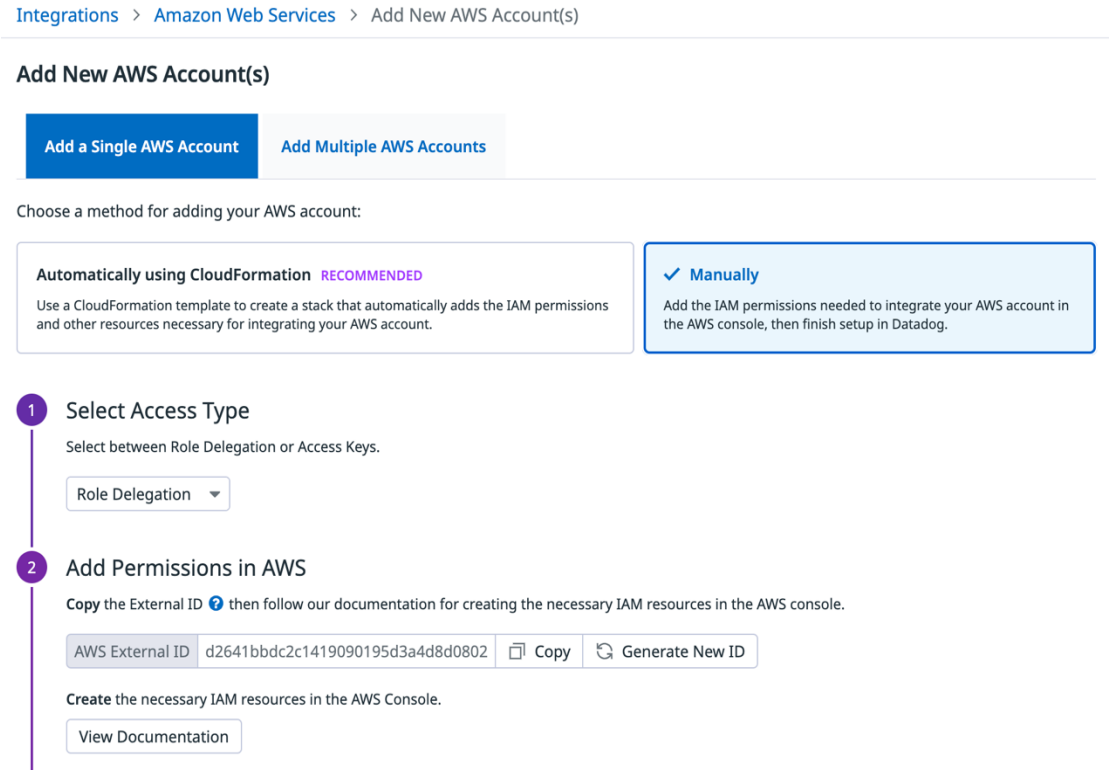


Figure 4.93. Integrate Datadog with AWS

After all step are finished, all the services from AWS are ready to monitor as shown in Figure 4.94.

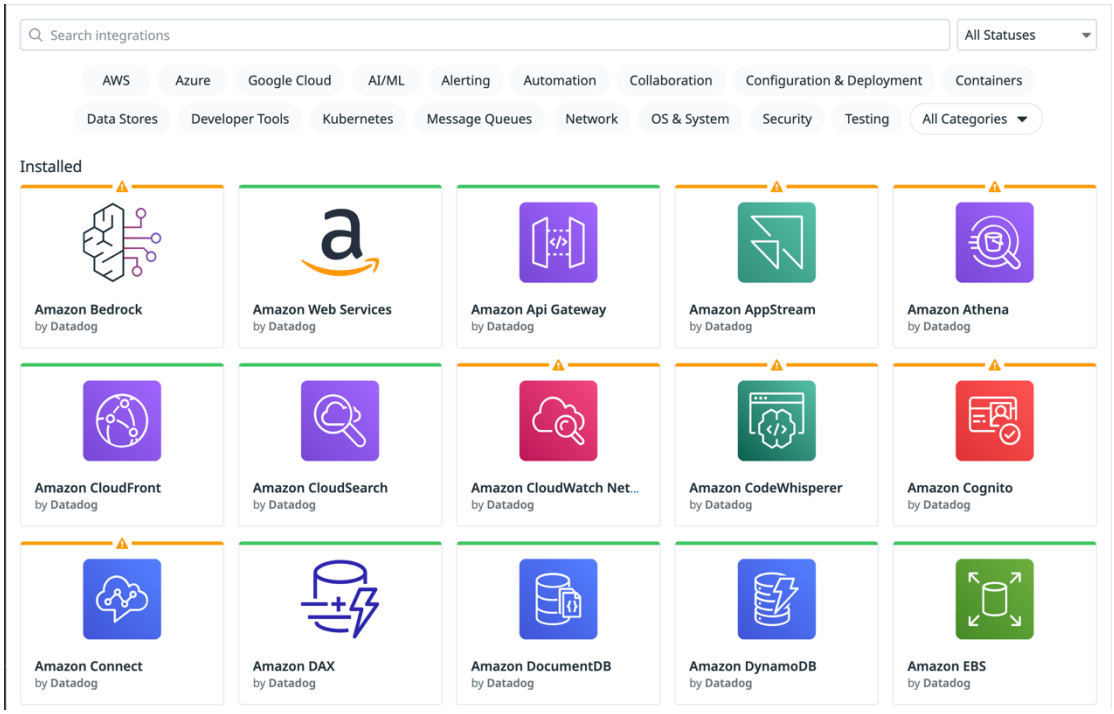


Figure 4.94. Integrate Datadog with AWS

4.12. Testing and Validation

There are several methods to add data to Amazon S3. Figure 4.95 presents Amazon S3 console to add data using AWS management console.

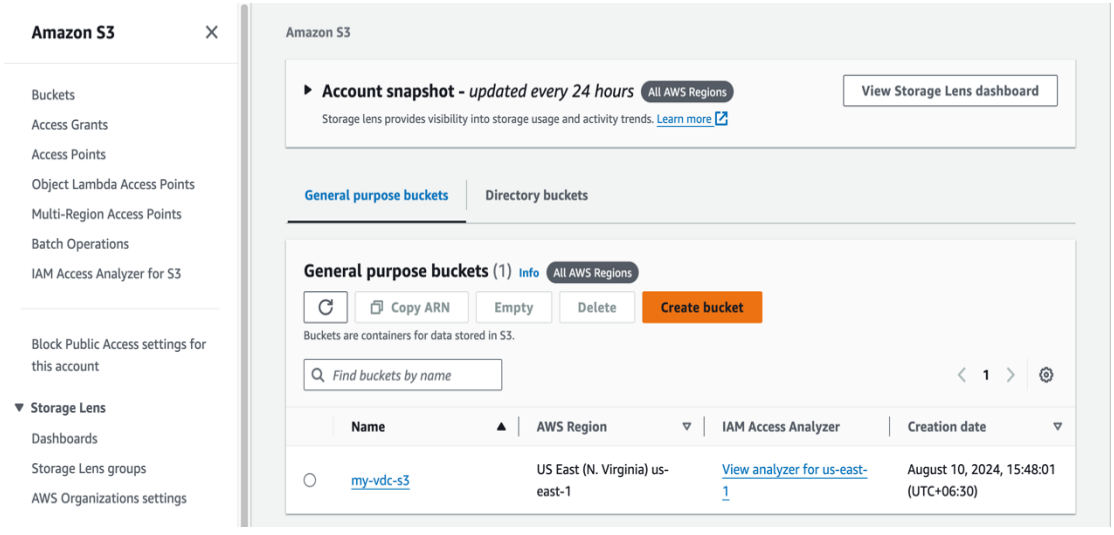


Figure 4.95. Testing and Validation

Navigate to the bucket where want to upload data and click on “Upload” as shown in Figure 4.96.

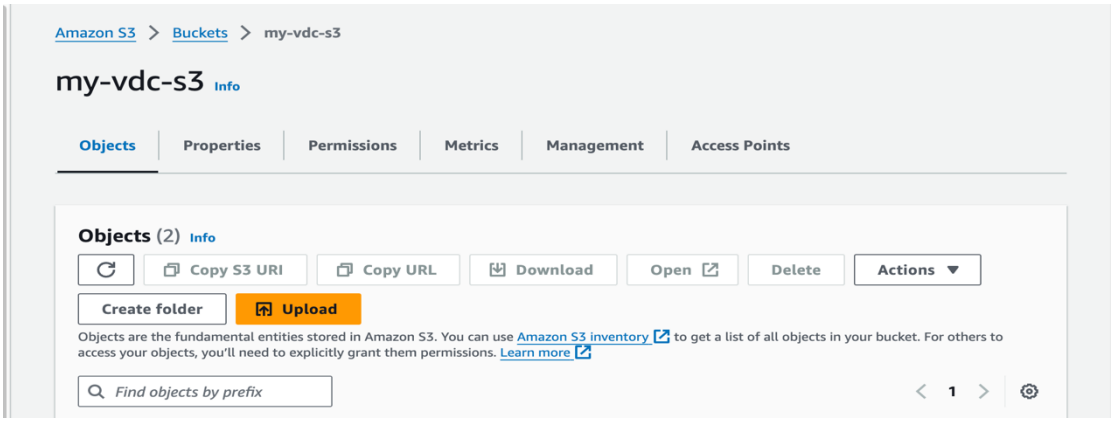


Figure 4.96. Testing and Validation

As presented in Figure 4.97, select files or folders form local machine to upload or also can drag and drop files directly into the S3 bucket from local machine.

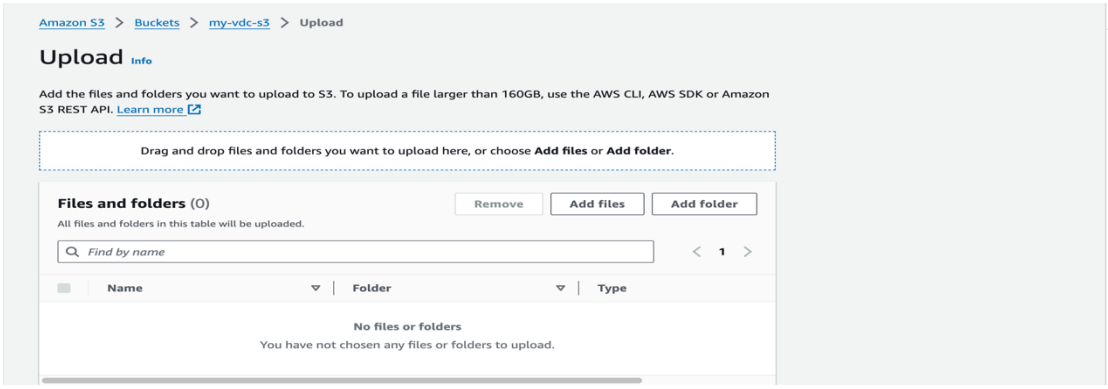


Figure 4.97. Testing and Validation

There are several methods to add data to DynamoDB. Figure 4.98 presents DynamoDB console to add data using AWS management console.

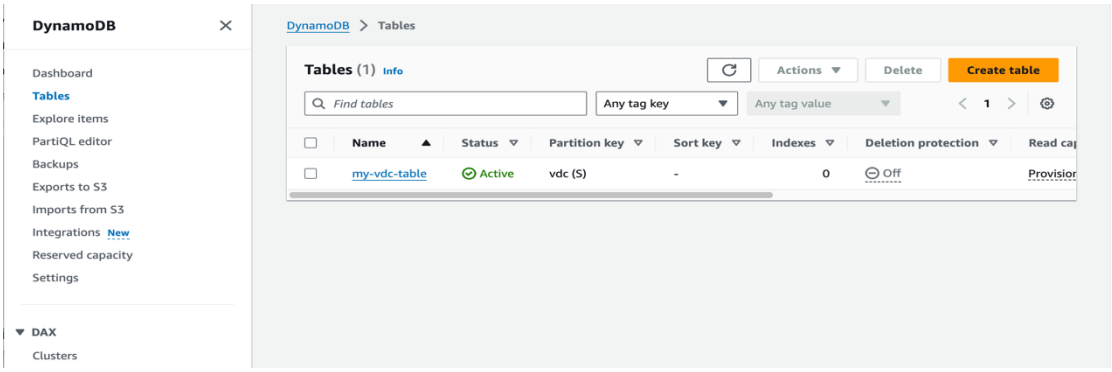


Figure 4.98. Testing and Validation

Click on “Explore items”, navigate the table where want to upload data and click on “Create item” button as demonstrated in Figure 4.99.

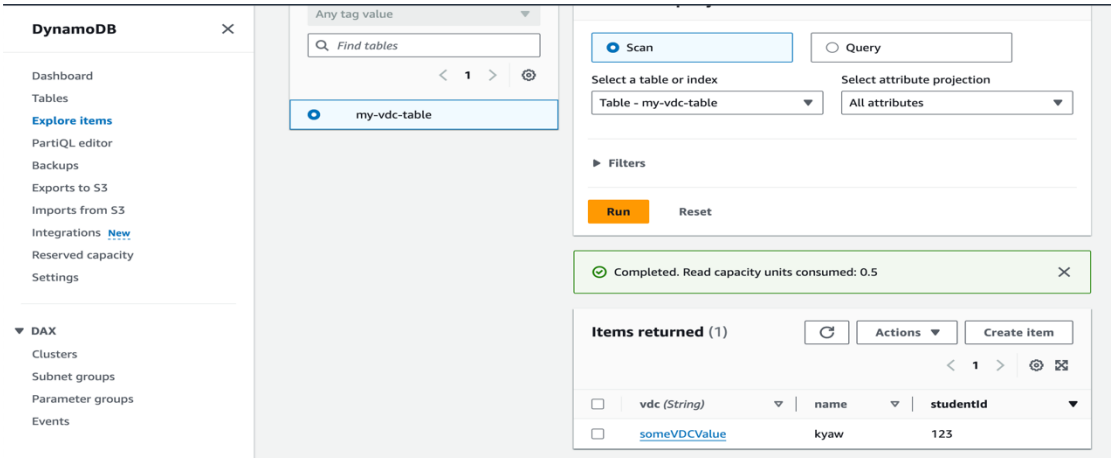


Figure 4.99. Testing and Validation

As shown in Figure 4.100 click on “Add new attribute” and select type.

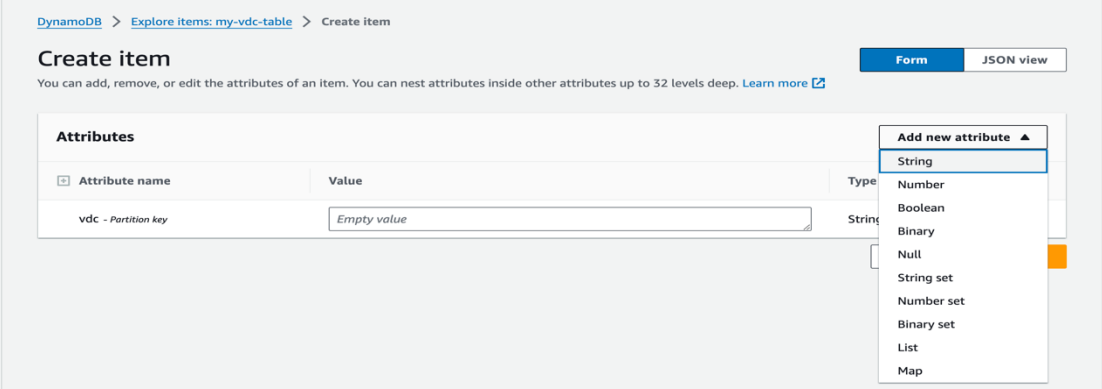


Figure 4.100. Testing and Validation

Fill the attribute name, value and click on “Add new attribute” again to add new attribute and click on “Create item” to create and save data as presented in Figure 4.101.

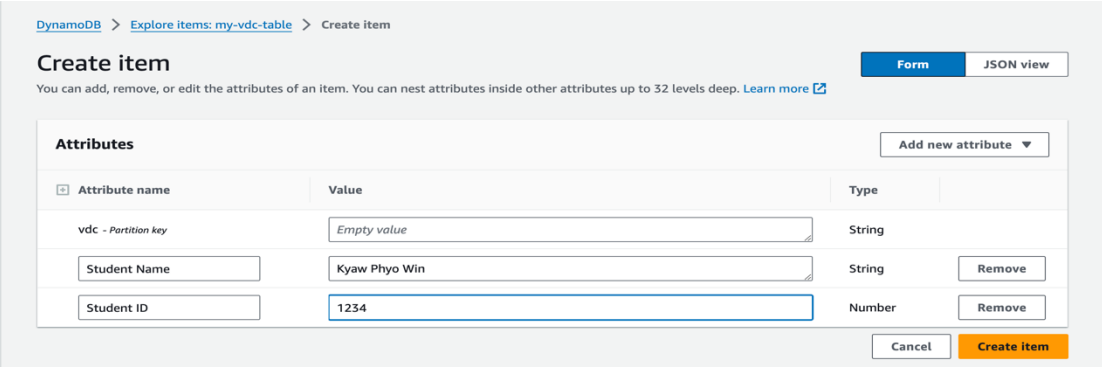


Figure 4.101. Testing and Validation

There are several methods to upload web files to EC2. Figure 4.102 presents step by step guide to add files to EC2 form github using Terminal (on MacOs) or

Command Prompt (on WindowOS). Connect to EC2 instance using SSH. Replace "your-key.pem" with private key file and "ec2-user@your-ec2-public-dns" with instance's public DNS.

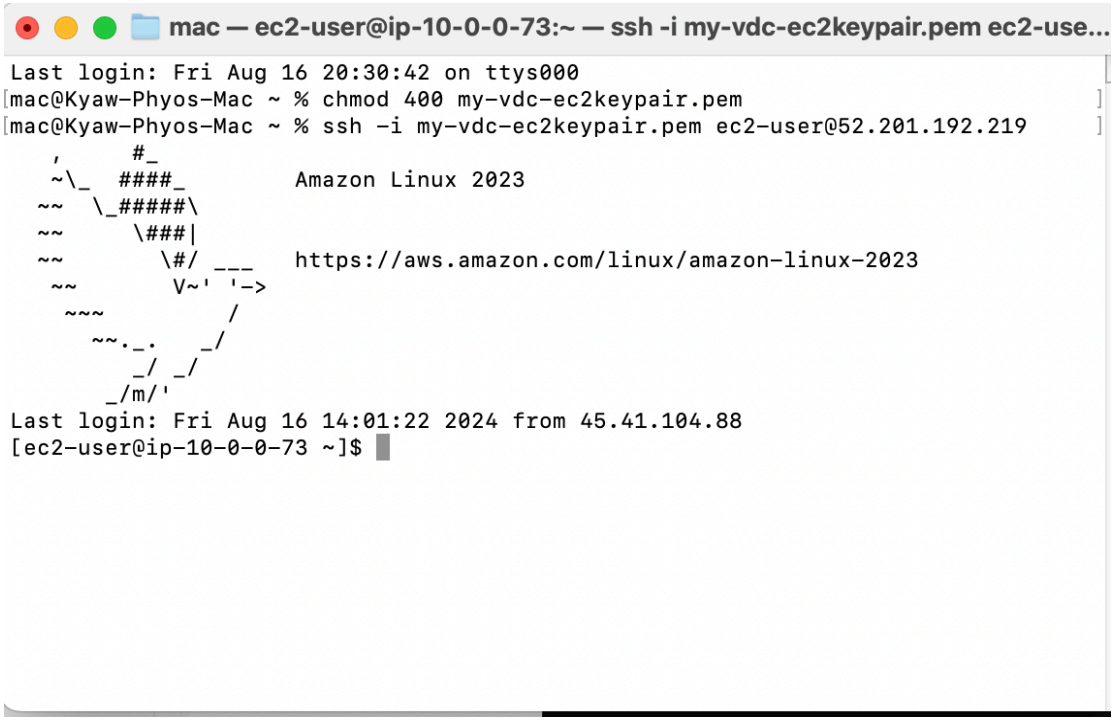


Figure 4.102. Testing and Validation

Depending on instance's Linux distribution, might use yum (for Amazon Linux/CentOS/RHEL) or apt-get (for Ubuntu/Debian) and to update the package list run commmand as shown in Figure 4.103.

For Amazon Linux or CentOS/RHEL:

```bash
sudo yum update -y
```

For Ubuntu/Debian:

```bash
sudo apt-get update
```

Figure 4.103. Testing and Validation

Run the command as presented in Figure 4.104 to install git to EC2.

For Amazon Linux/CentOS/RHEL:

```bash
sudo yum install git -y
```

For Ubuntu/Debian:

```bash
sudo apt-get install git -y
```

Figure 4.104. Testing and Validation

Navigate to the directory where want to clone as demonstrate in Figure 4.105.

```bash
cd /path/to/your/directory
```

Figure 4.105. Testing and Validation

As demonstrated in Figure 4.106 clone the repository to EC2. Replace https://github.com/username/repository.git with your repository URL.

```bash
git clone https://github.com/username/repository.git
```

Figure 4.106. Testing and Validation

Navigate to the cloned repository as shown in Figure 4.107. Replace "repository" with your repository directory.

```bash
cd repository
```

Figure 4.107. Testing and Validation

Depending on project, need to install additional dependencies. Figure 4.108 presents to install node.js for node.js projects.

```bash
sudo yum install nodejs npm -y  # Amazon Linux/CentOS/RHEL
sudo apt-get install nodejs npm -y  # Ubuntu/Debian
```

Figure 4.108. Testing and Validation

After installing dependencies, can typically start application using commands specific to technology stack as shown in Figure 4.109.

```bash
npm start
```

Figure 4.109. Testing and Validation

Figure 4.110 demonstrates example web page running on EC2.

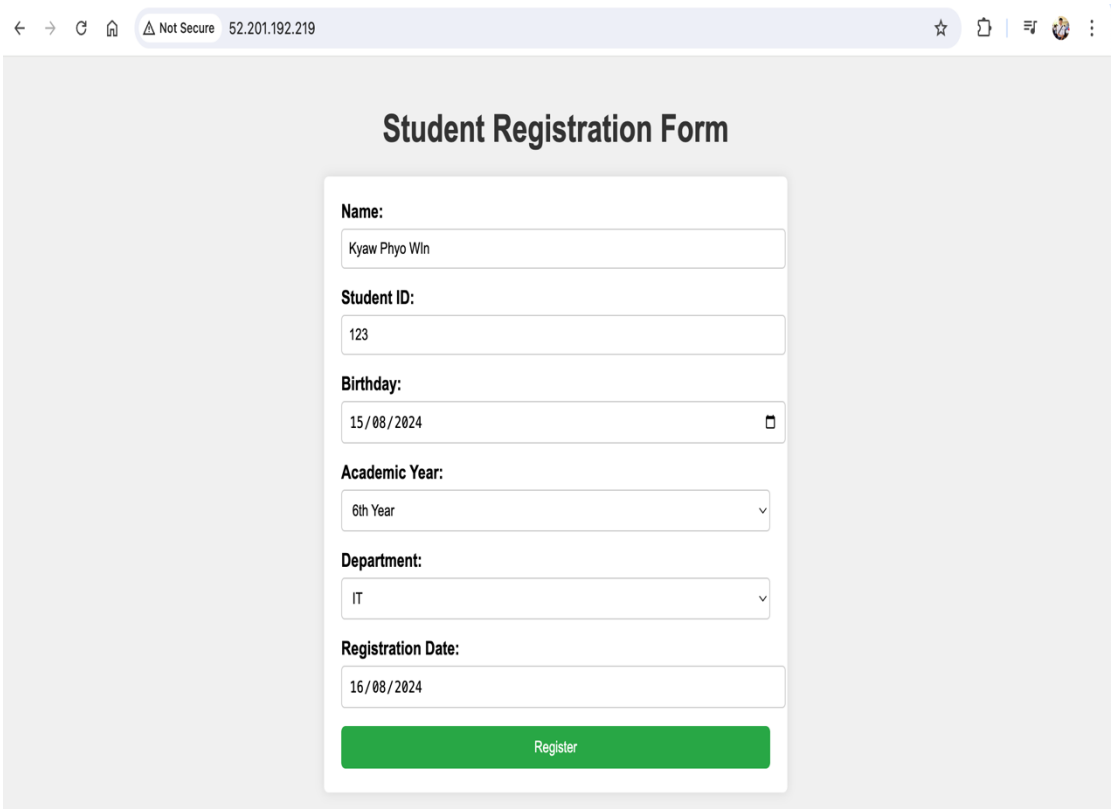


Figure 4.110. Testing and Validation

Figure 4.111 presents monitoring dashboard for EC2.

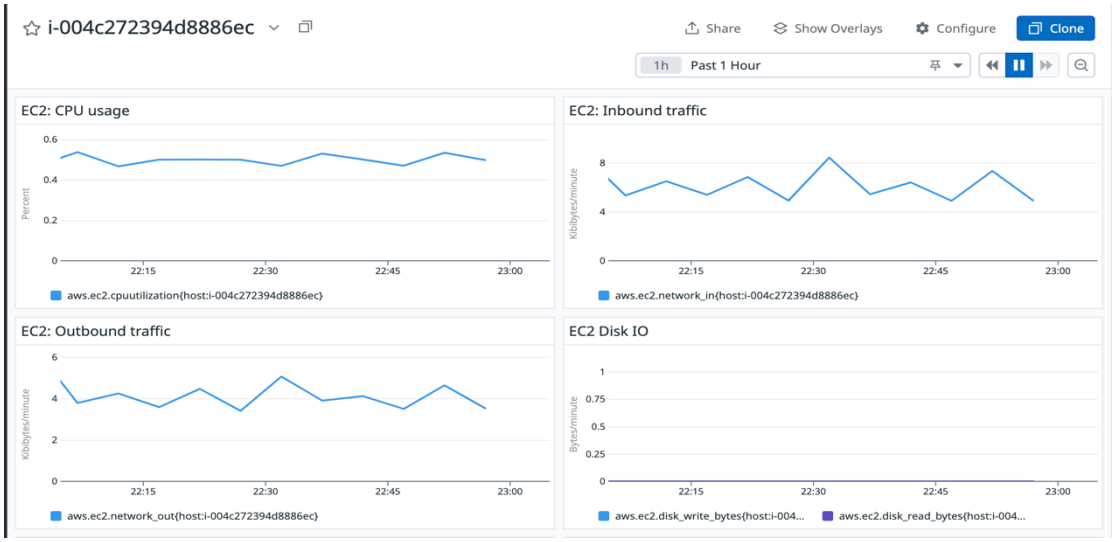


Figure 4.111. Testing and Validation

Figure 4.112 presents monitoring dashboard for EC2.

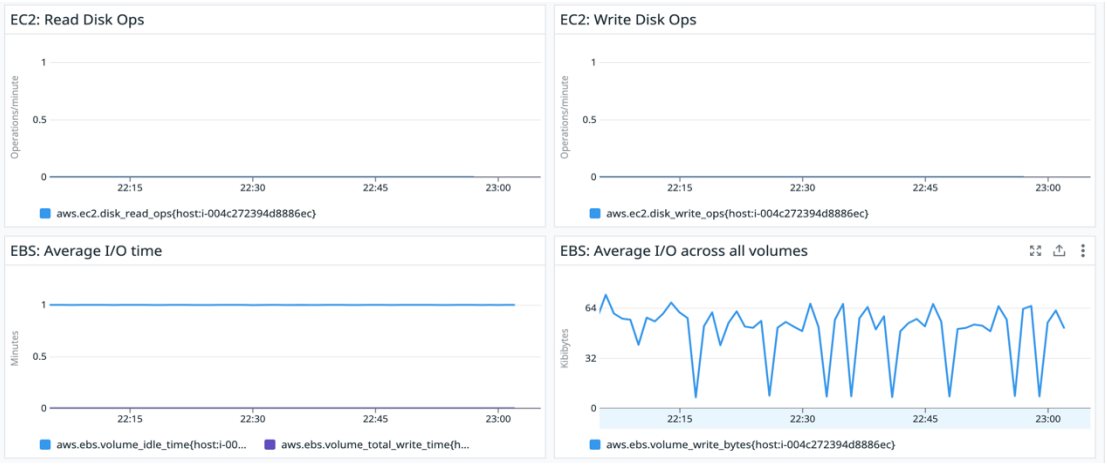


Figure 4.112. Testing and Validation

Figure 4.113 presents monitoring dashboard for EC2.

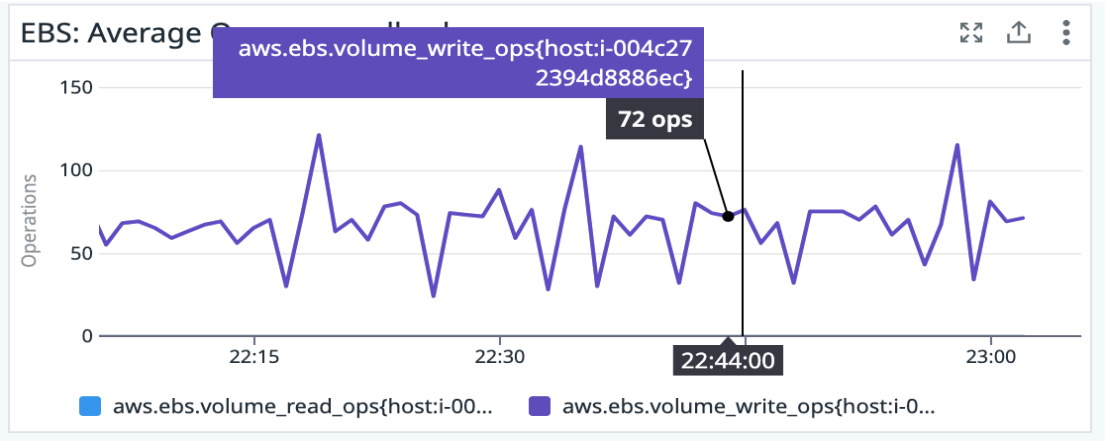


Figure 4.113. Testing and Validation