

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 Multi-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.

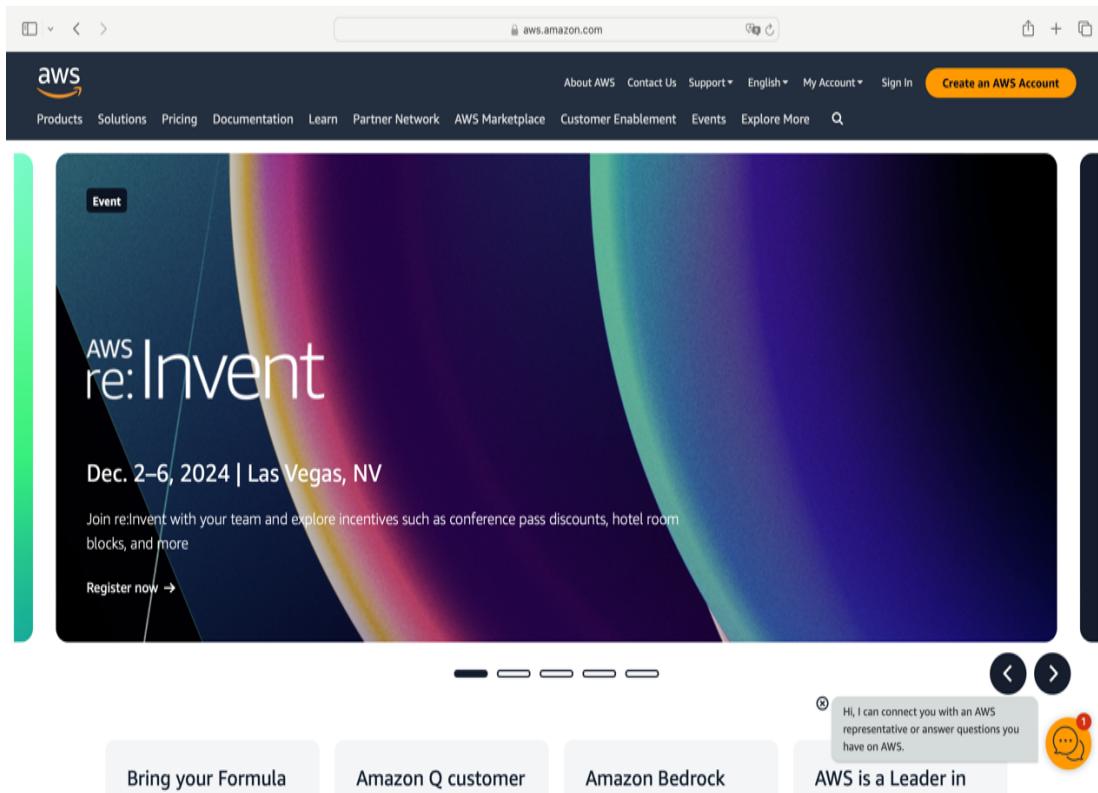


Figure 4.1. Creating AWS Account

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

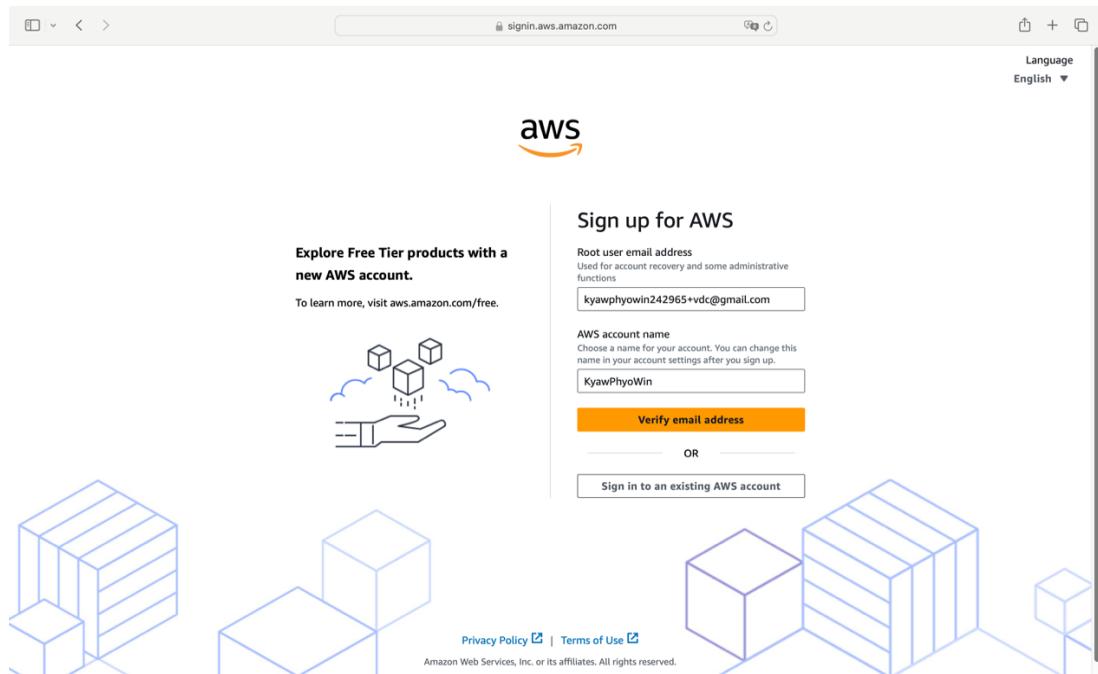


Figure 4.2. Creating AWS Account

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

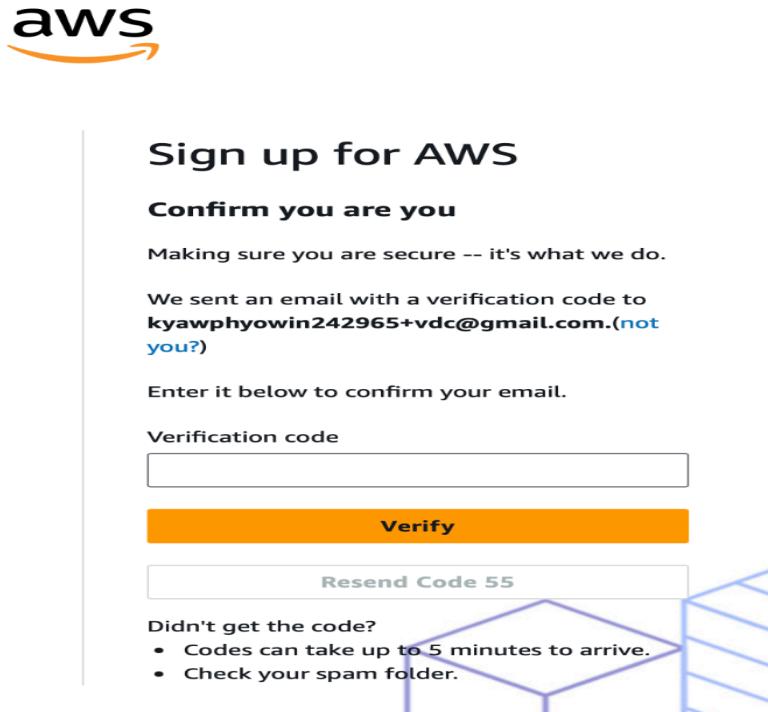


Figure 4.3. Creating AWS Account

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

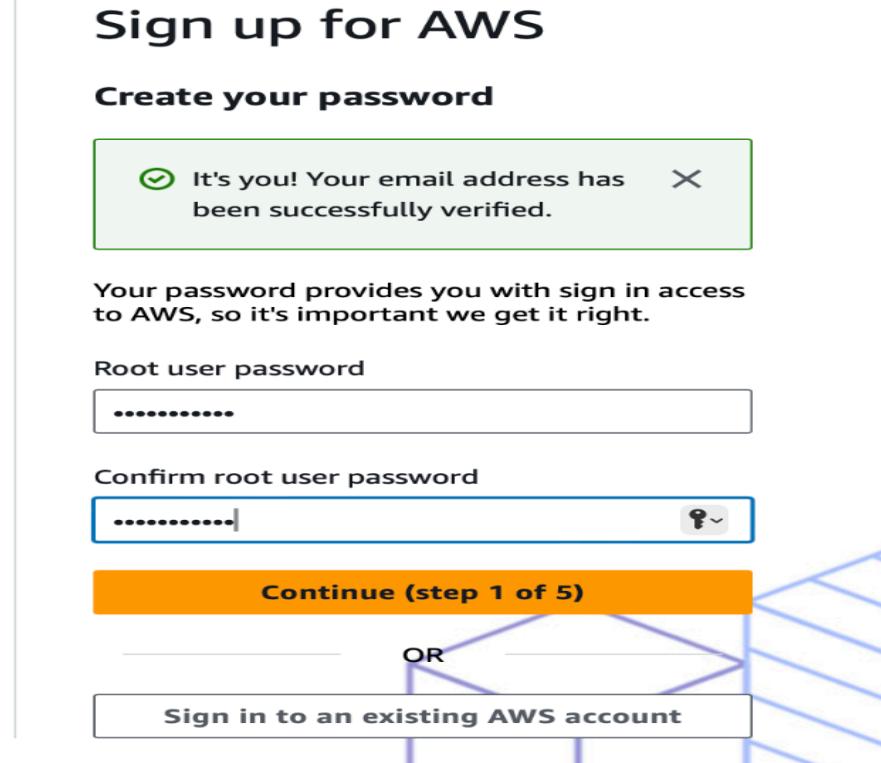


Figure 4.4. Creating AWS Account

Enter payment information as demonstrated in Figure 4.5.

Sign up for AWS

Billing Information

Credit or Debit card number

AWS accepts most major credit and debit cards. To learn more about payment options, review our [FAQ](#)

Expiration date

Security code (i)

CVV/CVC

Cardholder's name

Billing address

Use my contact address
No (178), 13 street, Myinetharyar Quarter
Mawlamyine Mon 12011
MM

Use a new address

Verify and Continue (step 3 of 5)

Figure 4.5. Creating AWS Account

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

Sign up for AWS

Confirm your identity

Before you can use your AWS account, you must verify your phone number. When you continue, the AWS automated system will contact you with a verification code.

How should we send you the verification code?

- Text message (SMS)
- Voice call

Country or region code

Myanmar (+95)



Mobile phone number

9754400705

Security check

	<input style="width: 20px; height: 20px; border: 1px solid #ccc;" type="text"/> ? <input style="width: 20px; height: 20px; border: 1px solid #ccc;" type="text"/> ?
--	--

Type the characters as shown above

zd77f2

Send SMS (step 4 of 5)

Figure 4.6. Creating AWS Account

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

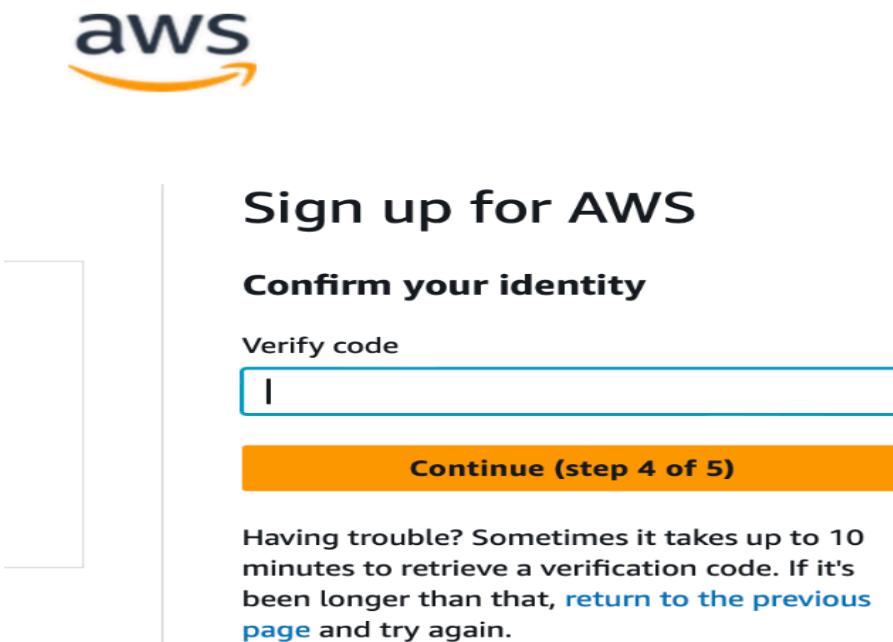


Figure 4.7. Creating AWS Account

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

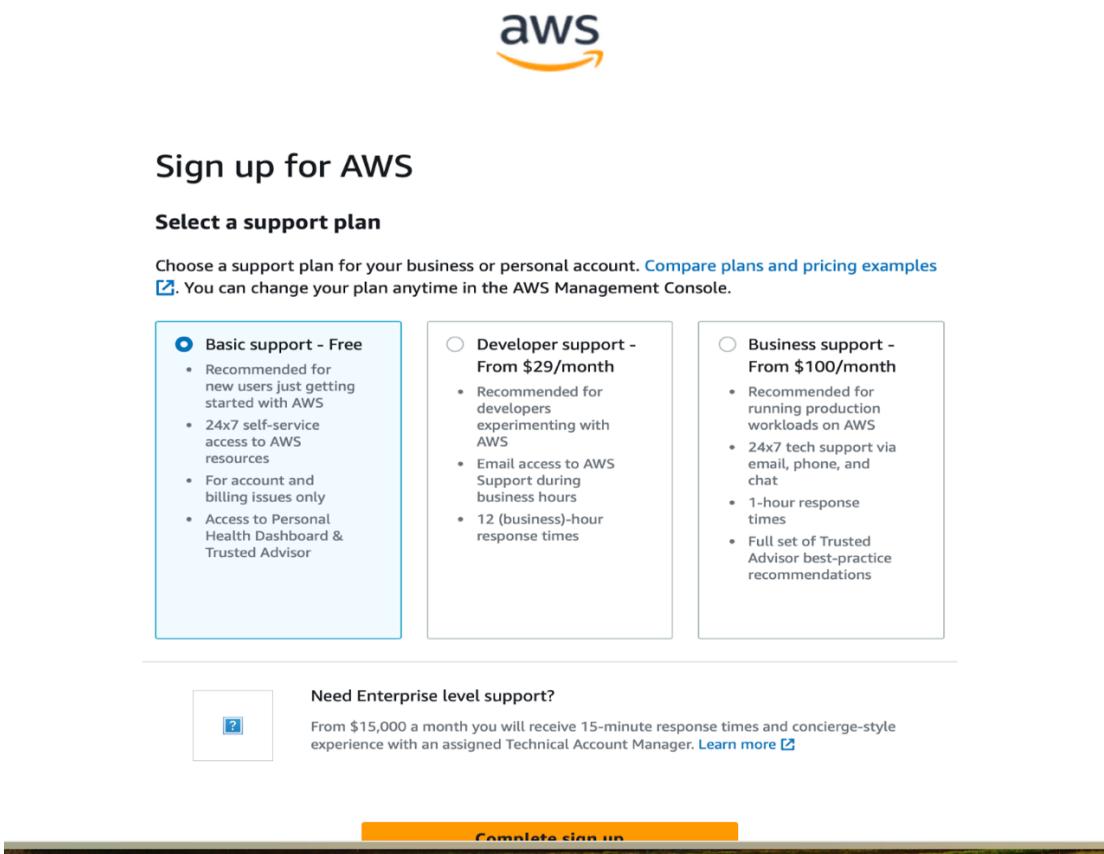


Figure 4.8. Creating AWS account

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.

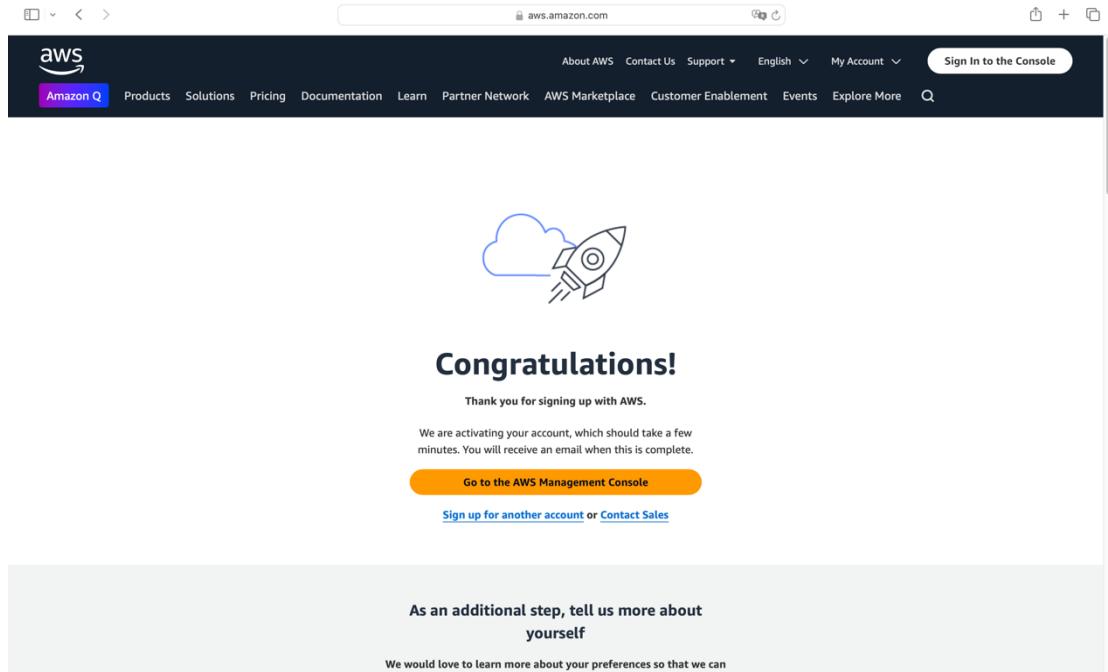


Figure 4.9. Creating AWS Account

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

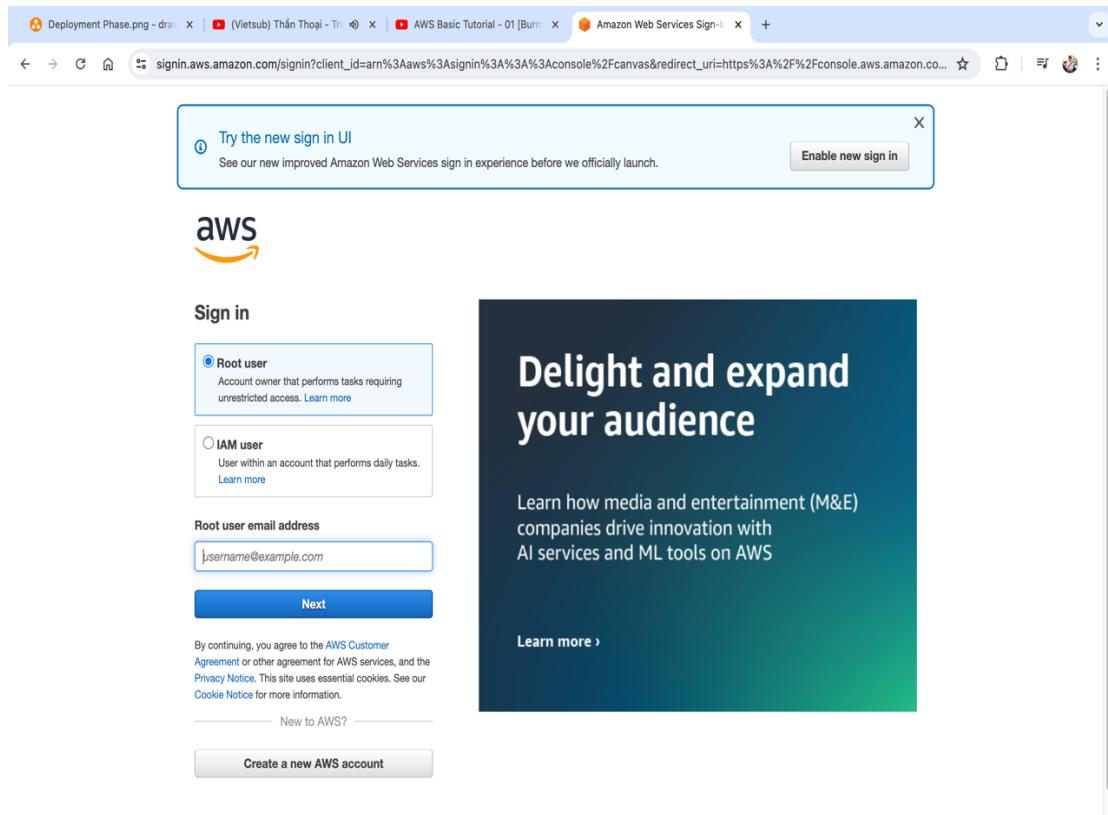


Figure 4.10. Sign up AWS Root User Account

Fill password for root user as shown in Figure 4.11.

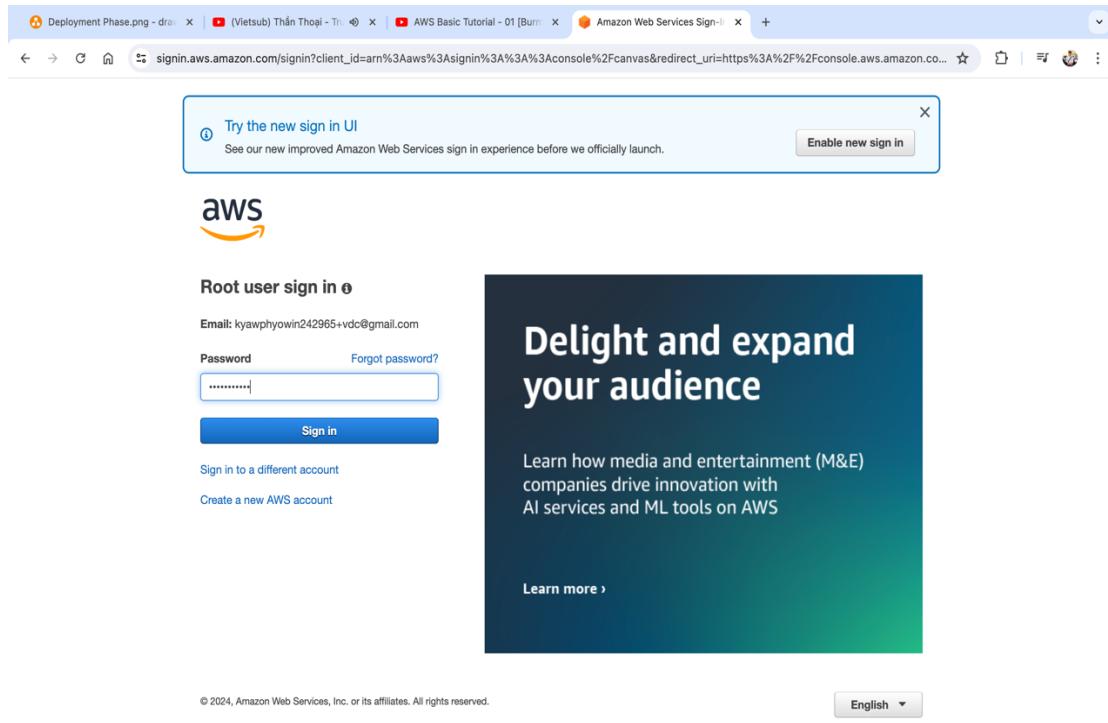


Figure 4.11. Sign up AWS Root User Account

Figure 4.12 displays the AWS management Console.

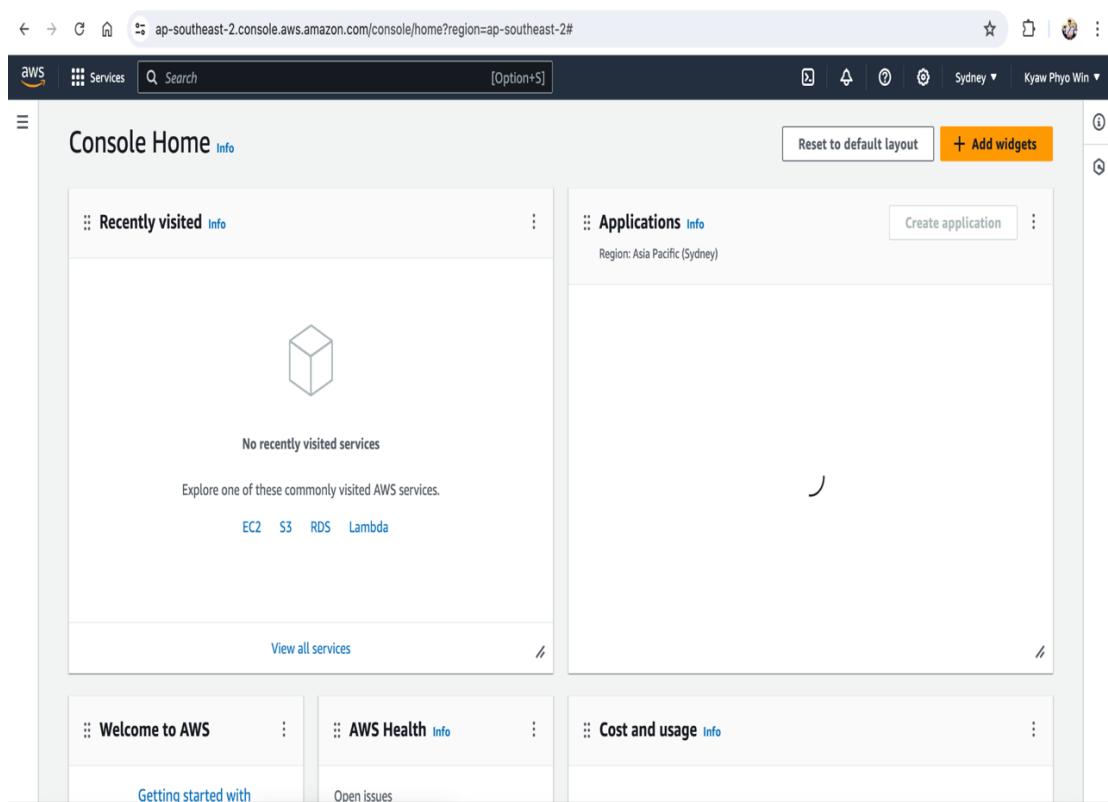


Figure 4.12. Sign up AWS Root User Account

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.

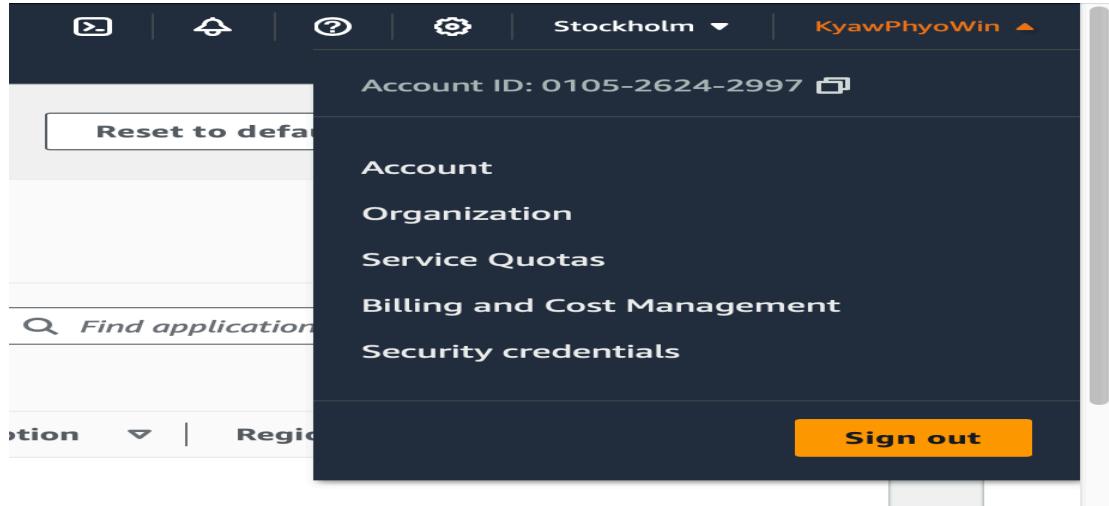


Figure 4.13. Assign MFA for Root User

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

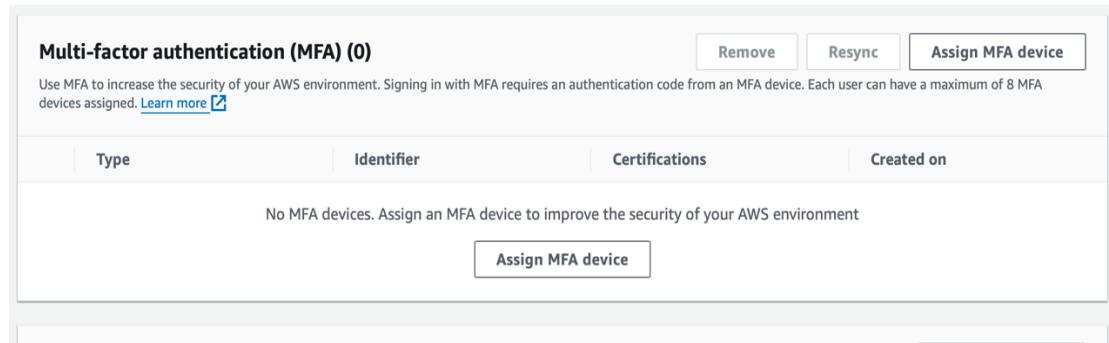


Figure 4.14. Assign MFA for Root User

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

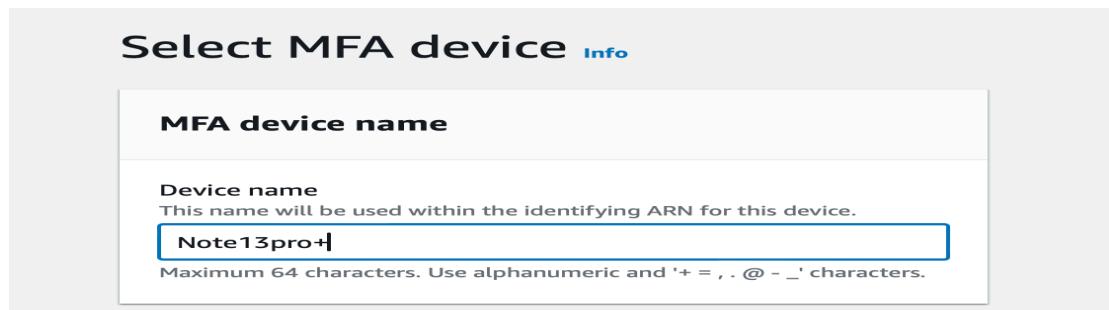


Figure 4.15. Assign MFA for Root User

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.

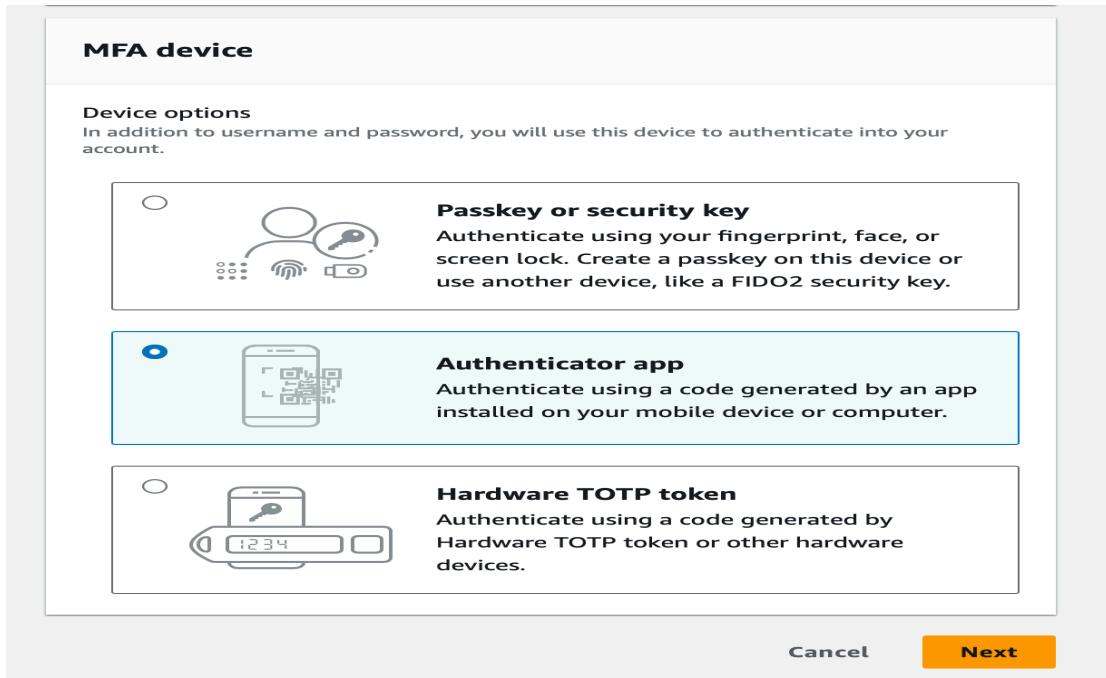


Figure 4.16. Assign MFA for Root User

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

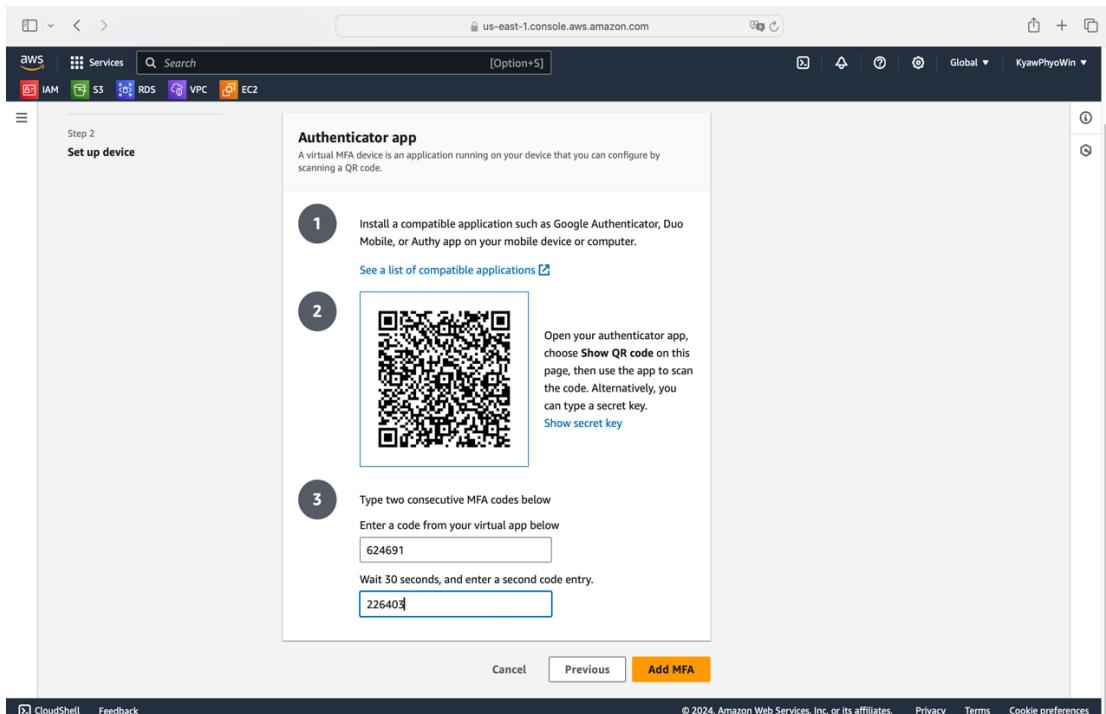


Figure 4.17. Assign MFA for Root User

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

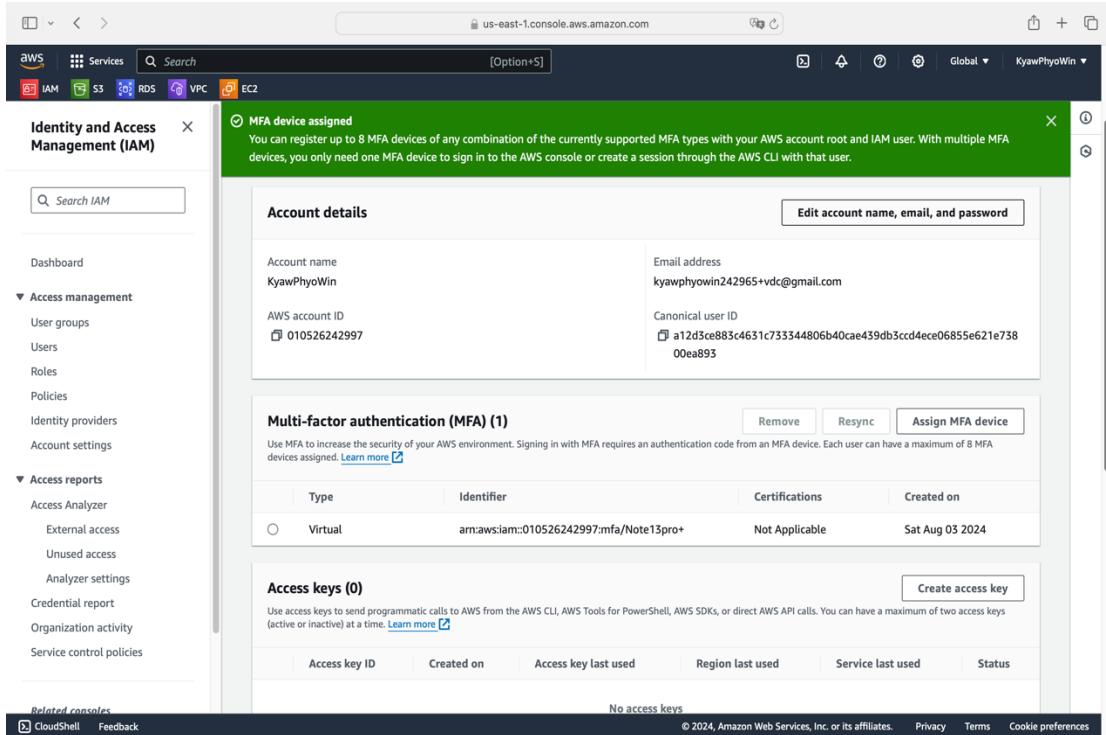


Figure 4.18. Assign MFA for Root User

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.

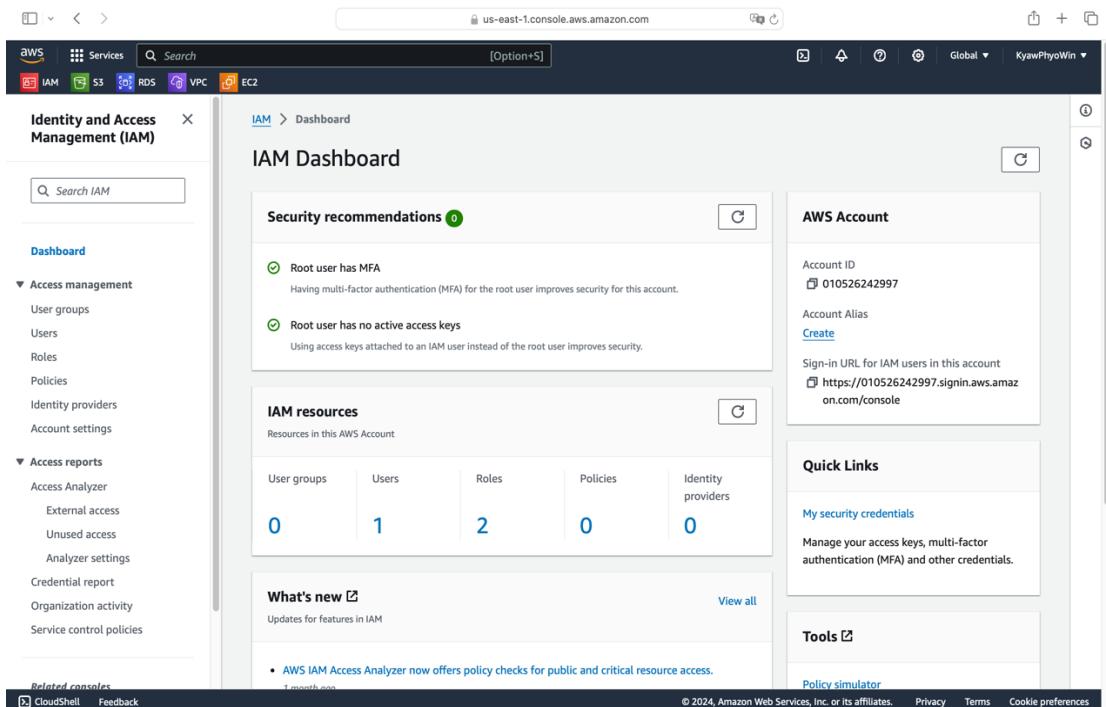


Figure 4.19. Create Account Alias

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

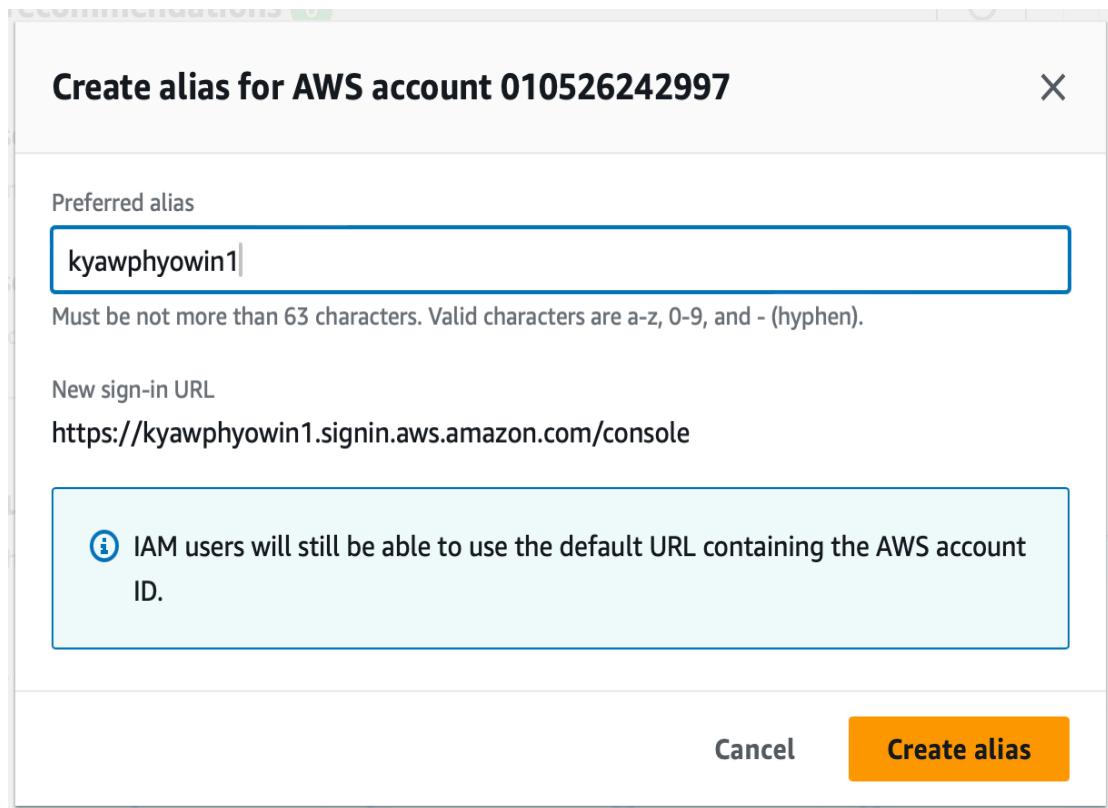


Figure 4.20. Create Account Alias

Figure 4.21 shows alias creation is completed successfully.

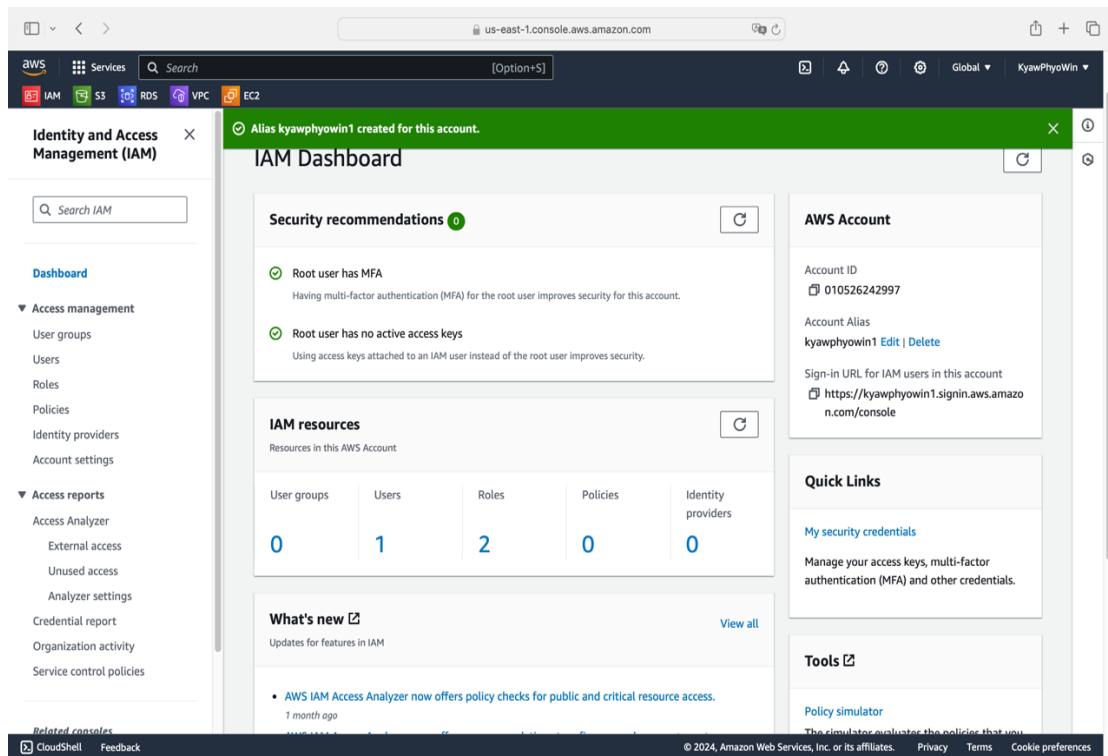


Figure 4.21. Create Account Alias

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.

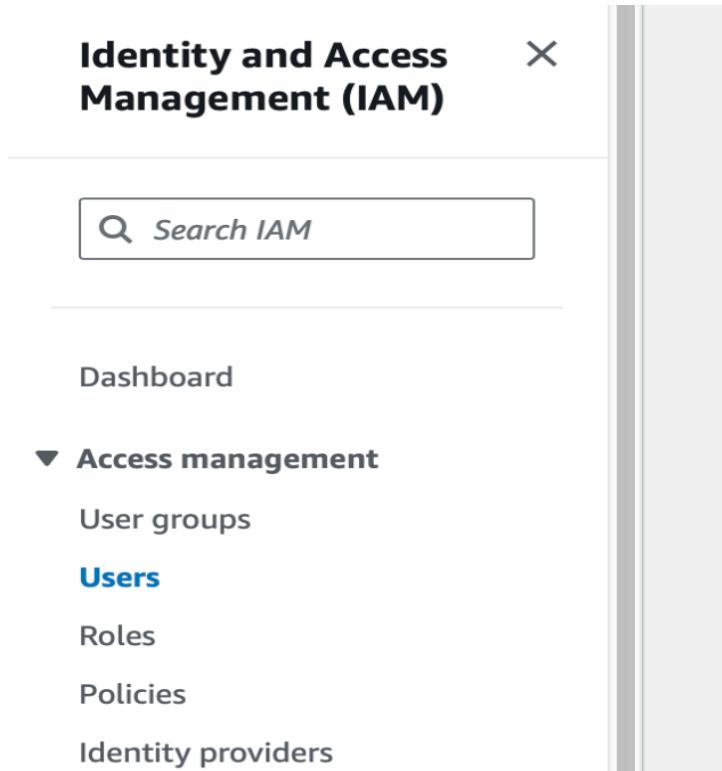


Figure 4.22. Creating IMA User

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

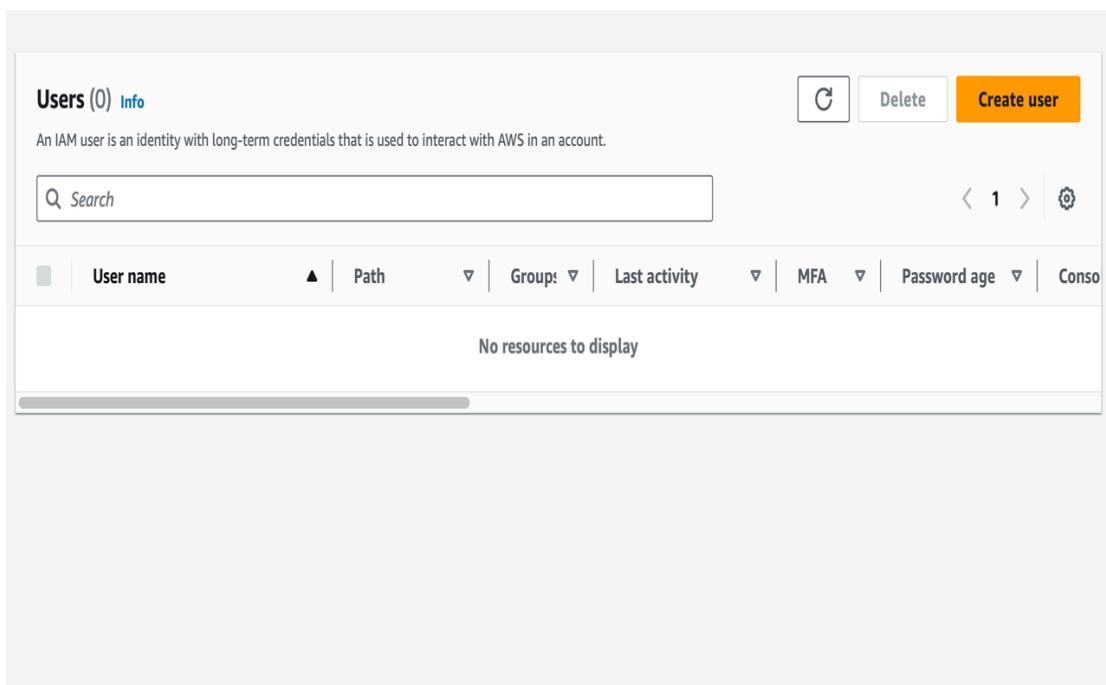


Figure 4.23. Creating IMA User

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”.

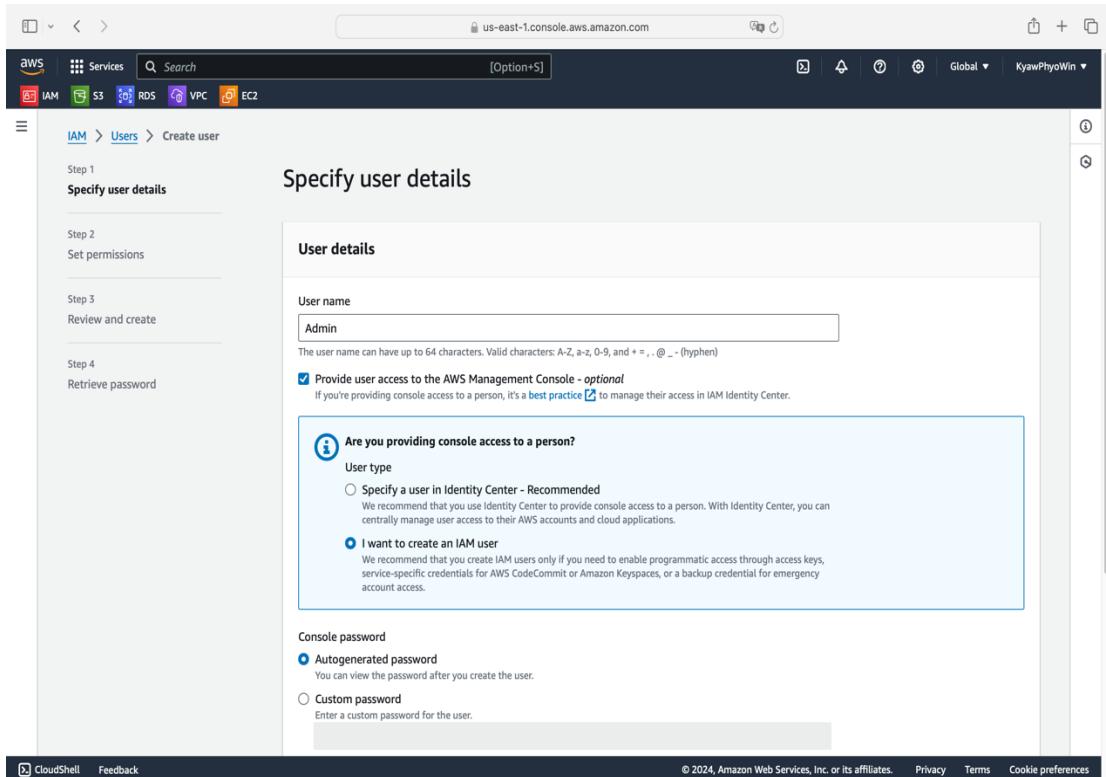


Figure 4.24. Creating IMA User

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

The screenshot shows the 'Specify user details' step of the IAM user creation wizard. The 'Custom password' option is selected, and a password '*****' is entered. A callout box highlights the note: 'If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)'.

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.

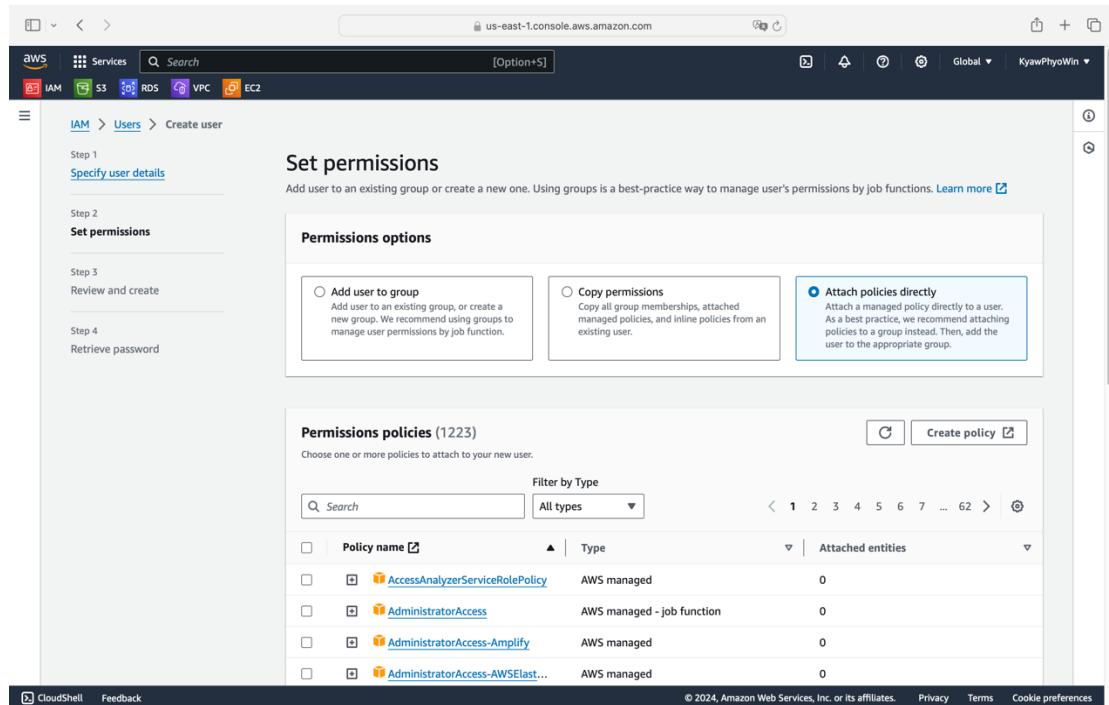


Figure 4.26. Creating IMA User

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

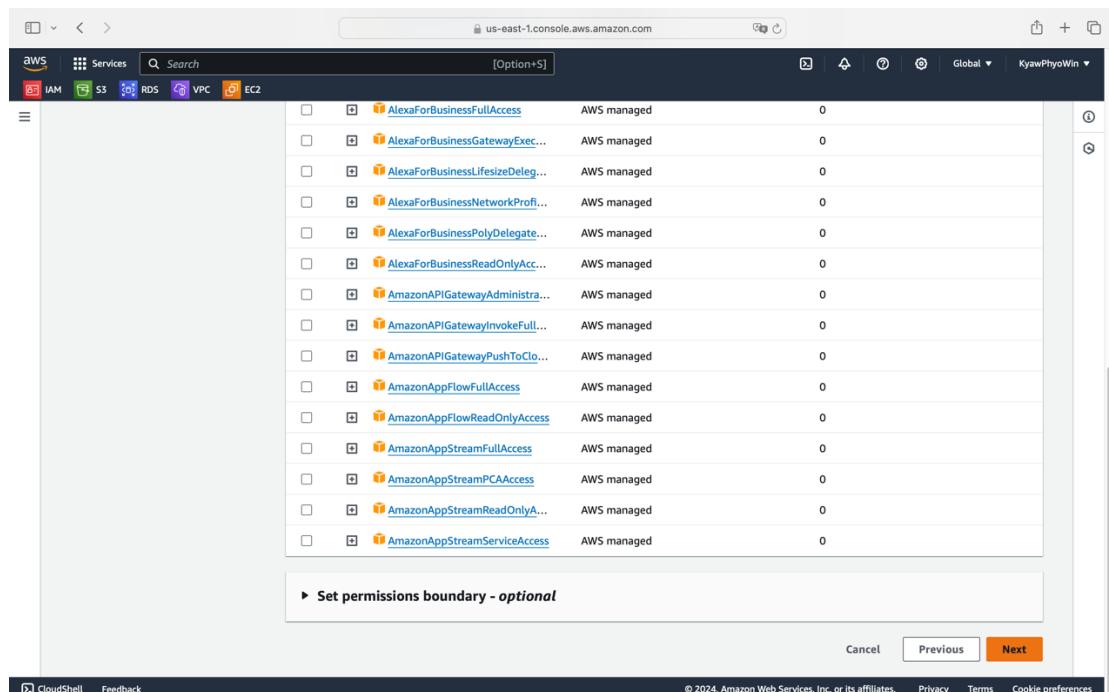


Figure 4.27. Creating IMA User

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

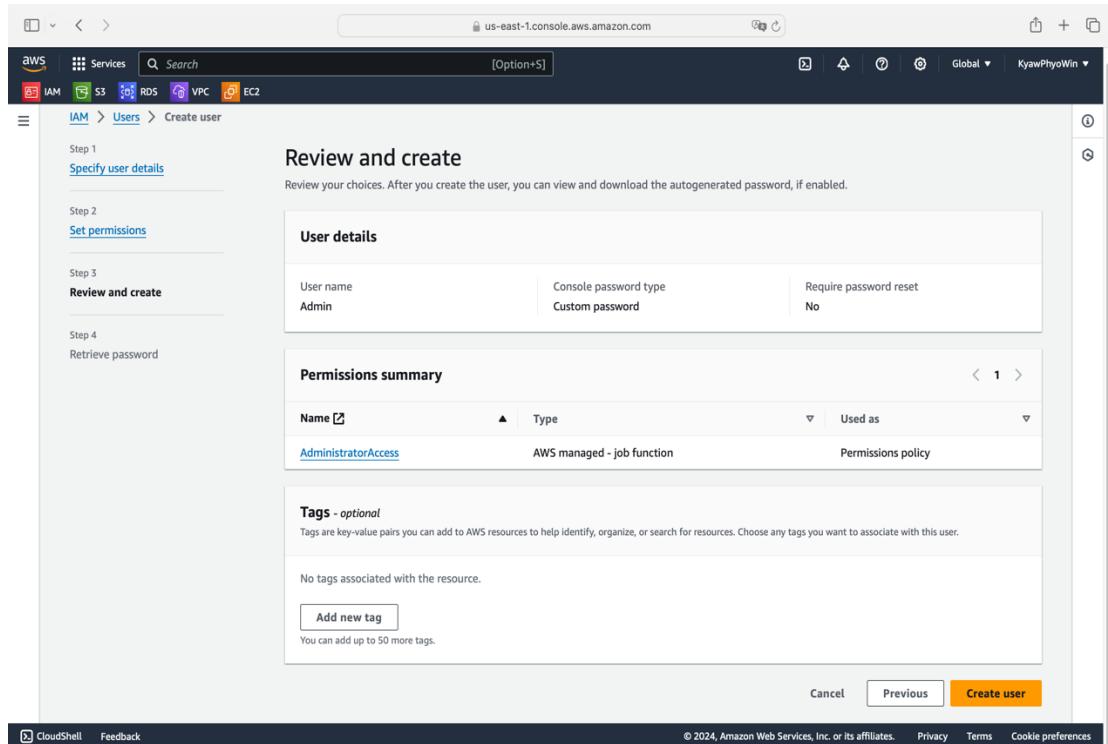


Figure 4.28. Creating IMA User

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

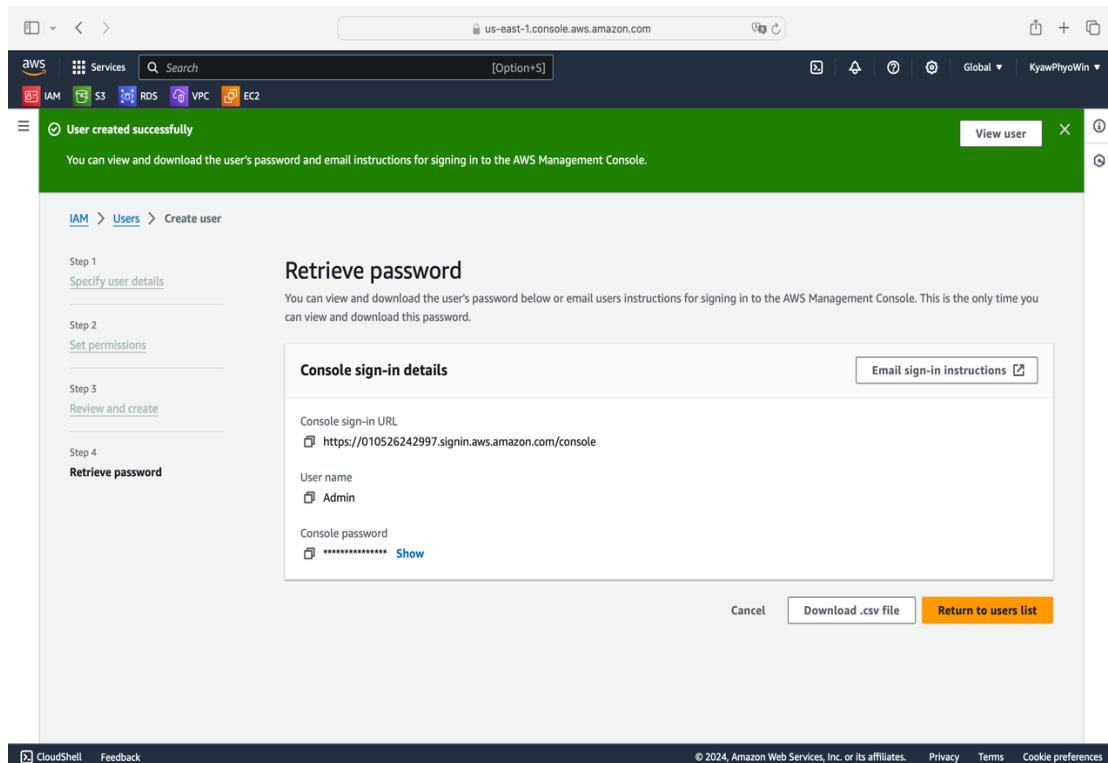


Figure 4.29. Creating IMA User

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.

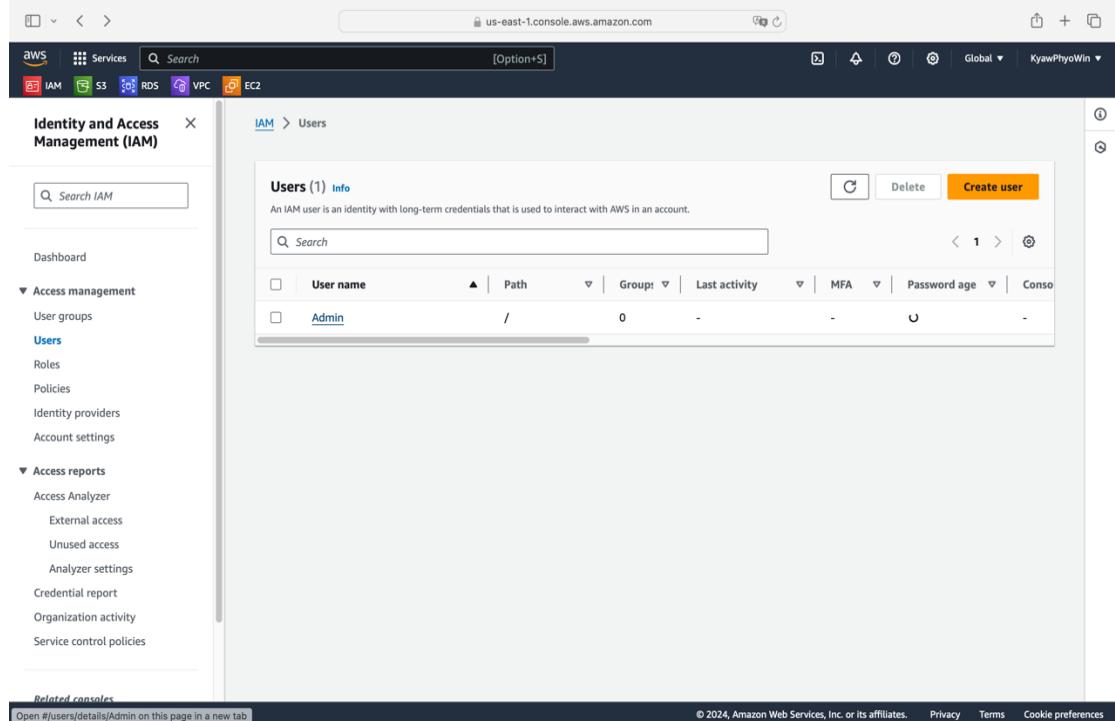


Figure 4.30. Assign MFA for IMA User

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.

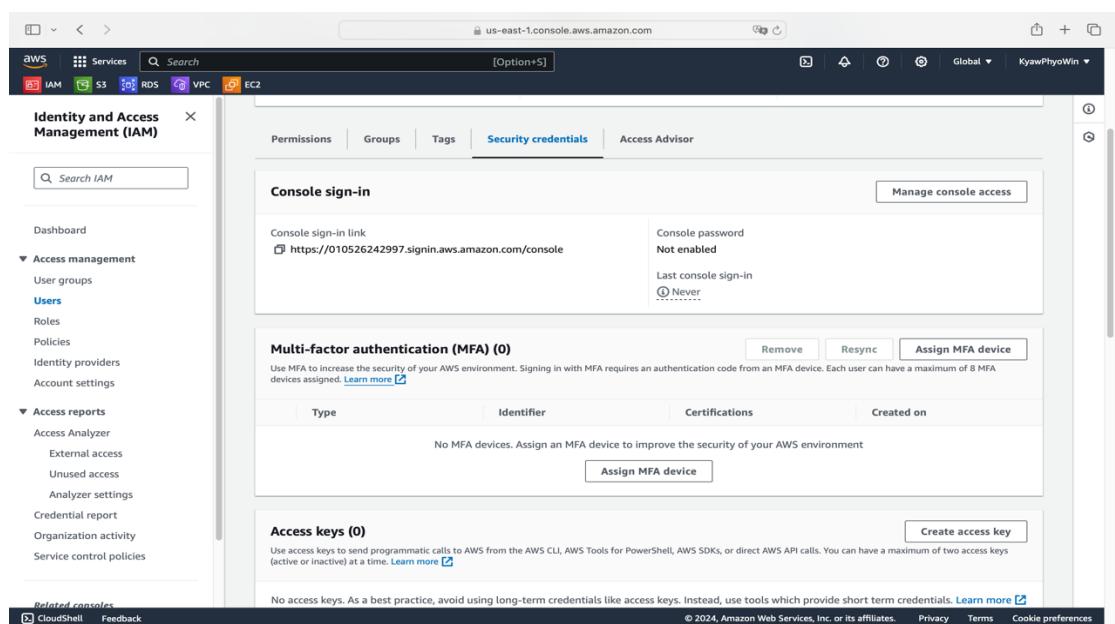


Figure 4.31. Assign MFA for IMA User

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 IAM user and enter account alias.

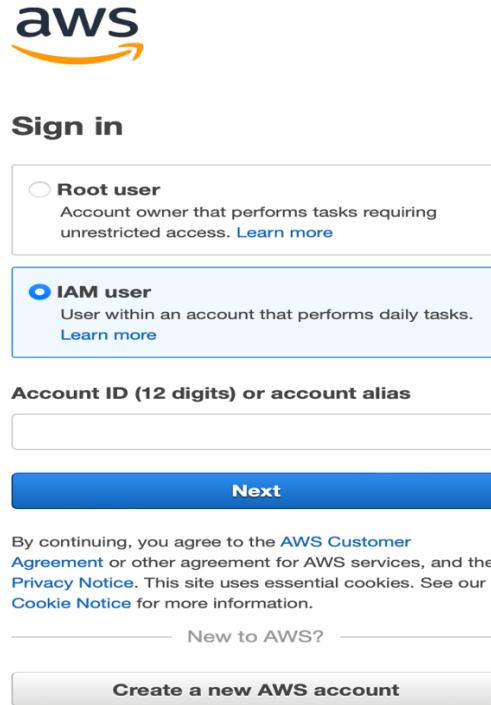


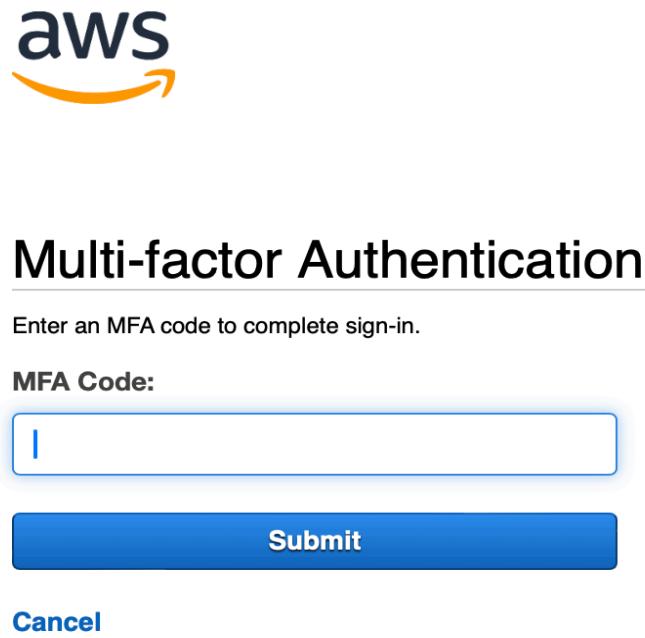
Figure 4.32. Verify MFA as IAM User

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

The screenshot shows the 'Sign in as IAM user' interface. At the top is the AWS logo. Below it is a 'Sign in as IAM user' button. There are three input fields: 'Account ID (12 digits) or account alias' containing 'kyawphyowin1', 'IAM user name' (empty), and 'Password' (empty). Below the password field is a checkbox labeled 'Remember this account'. A large blue 'Sign in' button is at the bottom. At the very bottom are two links: 'Sign in using root user email' and 'Forgot password?'

Figure 4.33. Verify MFA as IAM User

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



The screenshot shows the AWS Multi-factor Authentication (MFA) sign-in page. At the top is the AWS logo. Below it, the heading "Multi-factor Authentication" is centered. A sub-instruction "Enter an MFA code to complete sign-in." follows. A text input field labeled "MFA Code:" contains a single character "I". To the right of the input field is a large blue "Submit" button. Below the "Submit" button is a "Cancel" link.

Figure 4.34. Verify MFA as IAM User

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

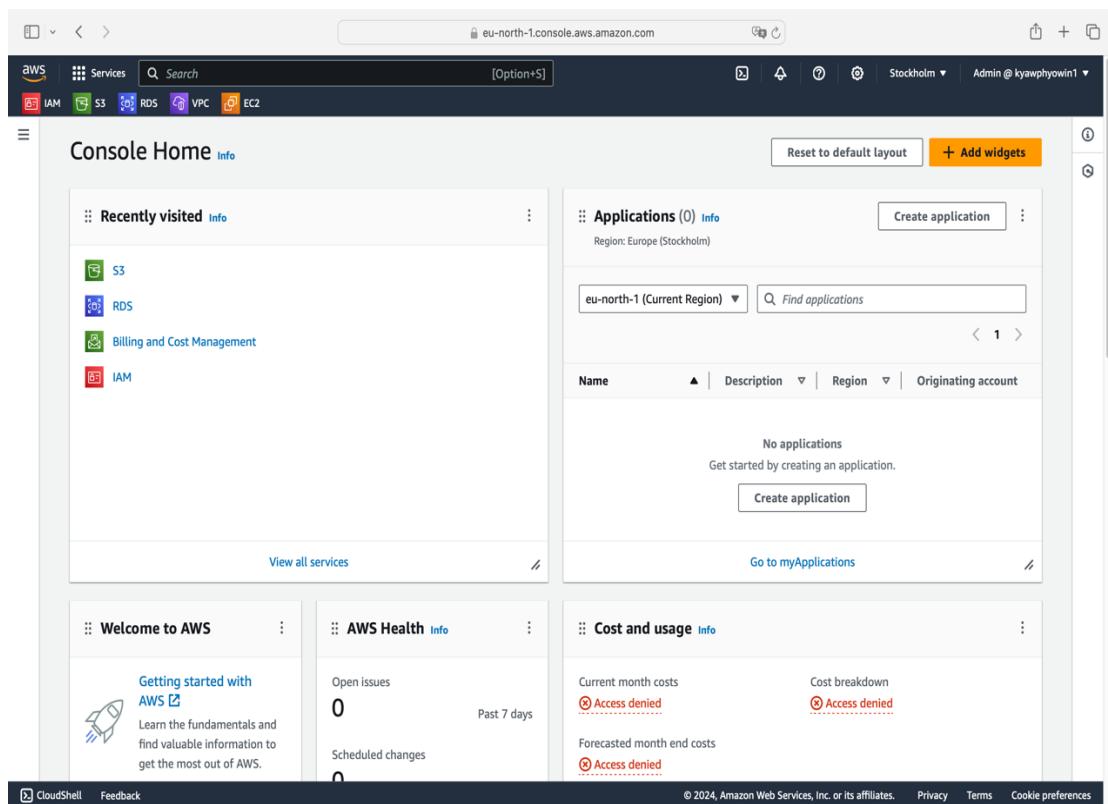


Figure 4.35. Verify MFA as IAM User

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.

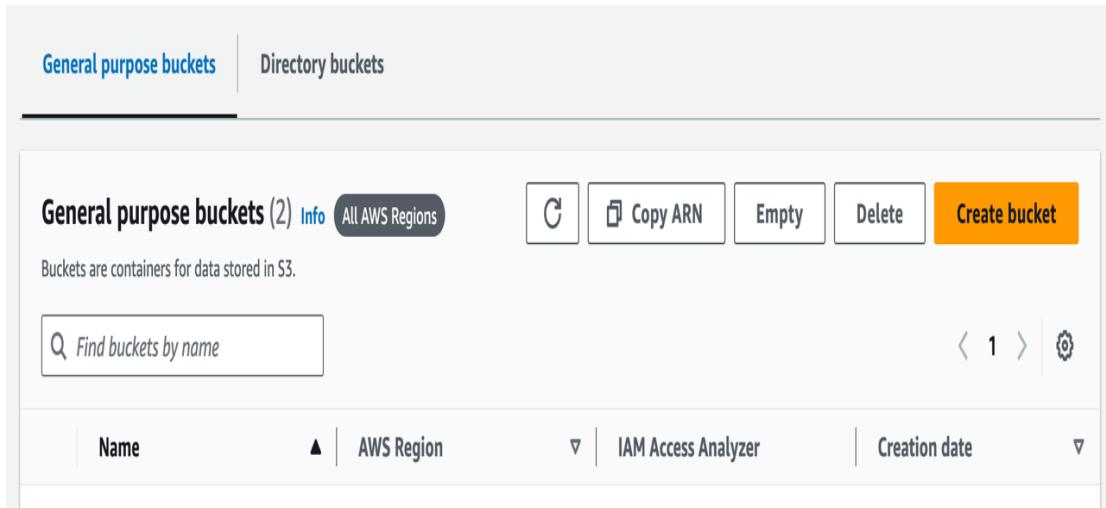


Figure 4.36. Configure S3

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

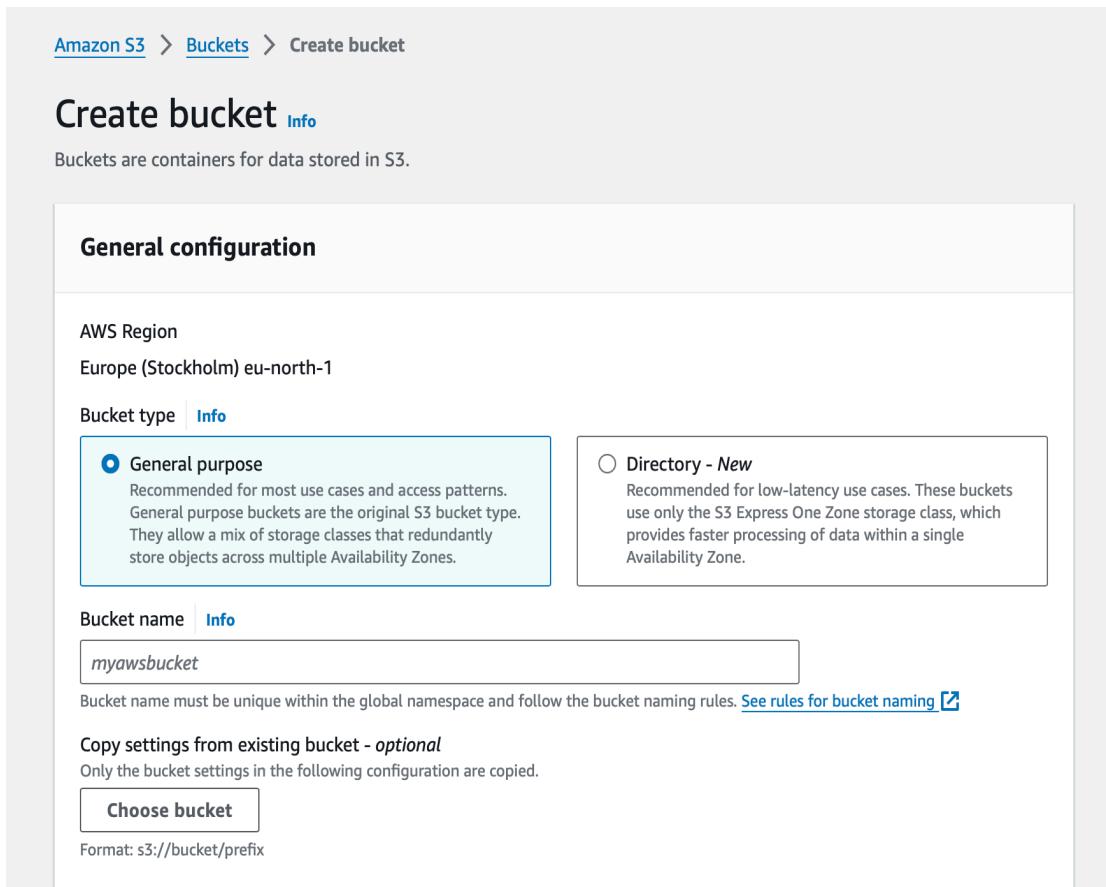


Figure 4.37. Configure S3

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

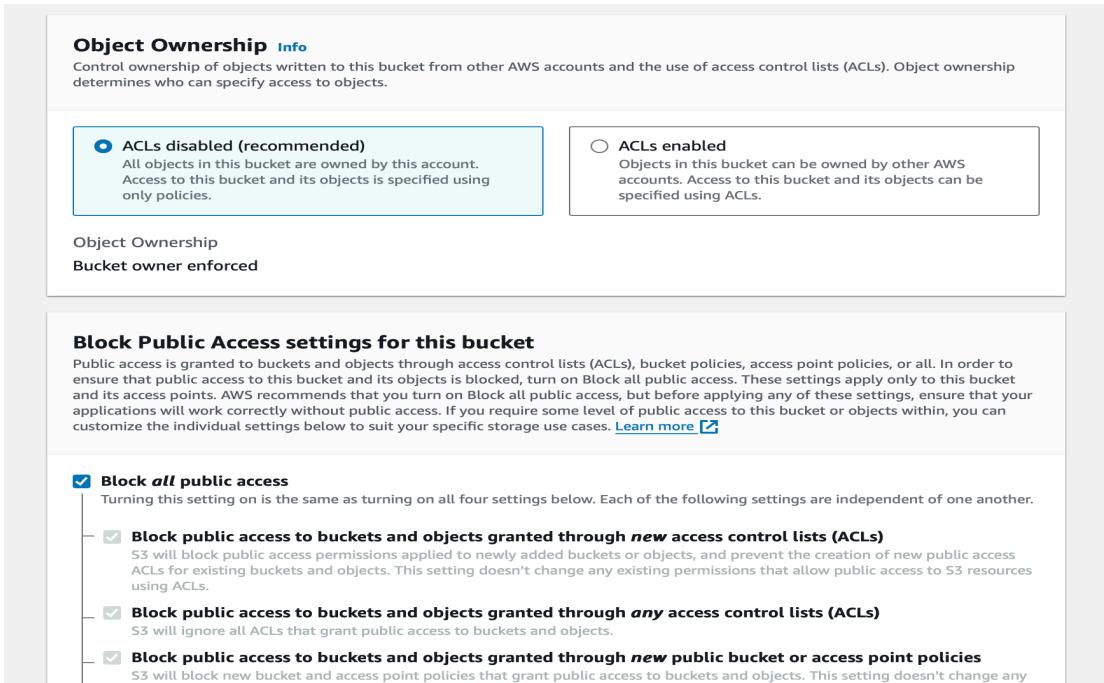


Figure 4.38. Configure S3

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

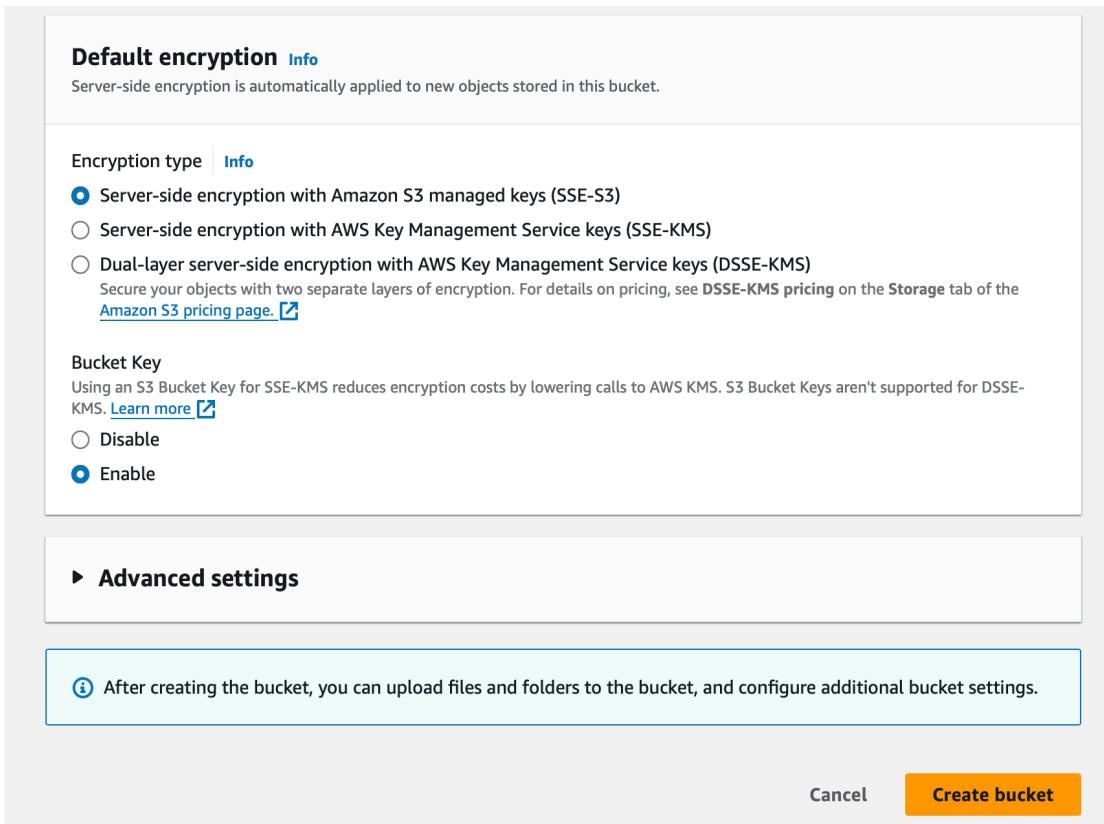


Figure 4.39. Configure S3

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

Name	AWS Region	IAM Access Analyzer	Creation date
my-vdc-bucket	Europe (Stockholm) eu-north-1	View analyzer for eu-north-1	August 3, 2024, 21:39:38 (UTC+06:30)

Figure 4.40. Configure S3

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

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access
⚠ Off
▶ Individual Block Public Access settings for this bucket

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

Figure 4.41. Configure S3

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

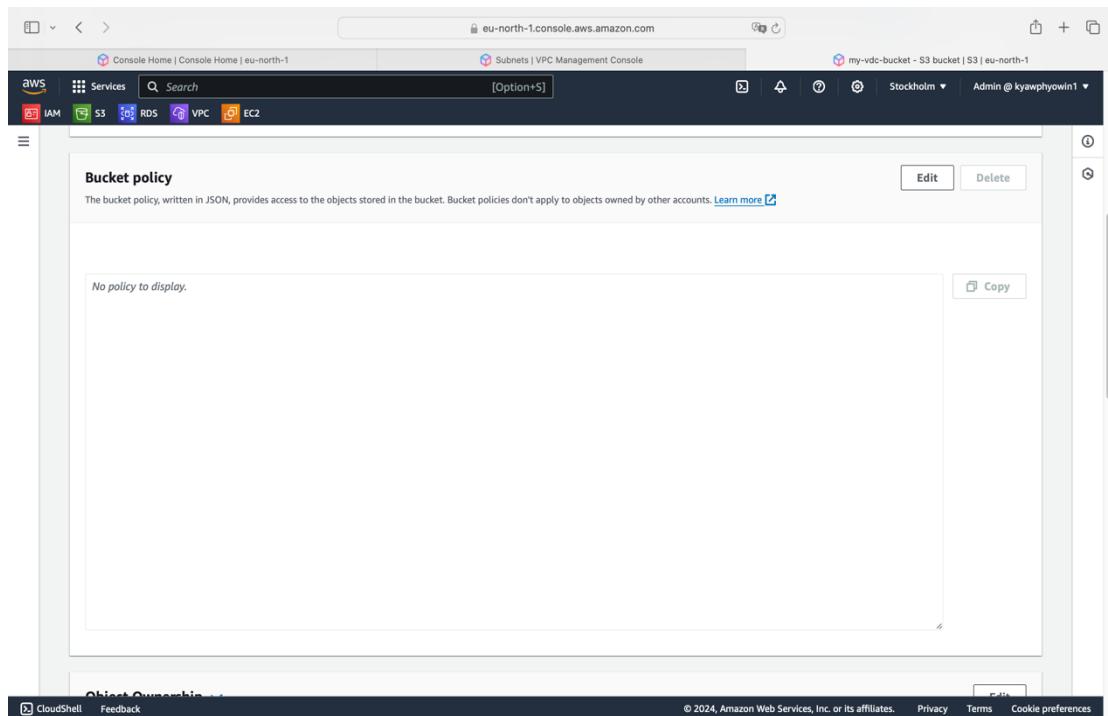


Figure 4.42. Configure S3

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

Policy

```

1  {
2      "Version": "2008-10-17",
3      "Statement":
4      {
5          "Sid": "AddPerm",
6          "Effect": "Allow",
7          "Principal": "*",
8          "Action": "s3:GetObject",
9          "Resource": "arn:aws:s3:::my-vdc-bucket"
10     }
11    },
12  }
13 }
14 }
15 }
16 }
```

Figure 4.43. Configure S3

As evidenced by Figure 4.44 S3 configuration is successfully complete.

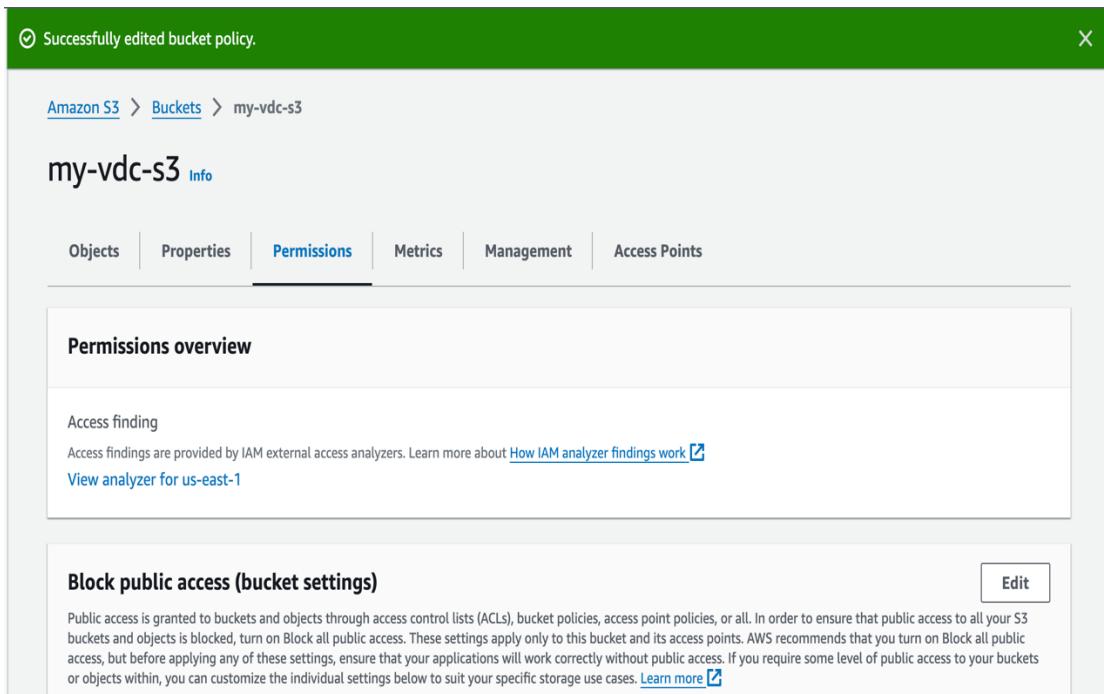


Figure 4.44. Configure S3

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.

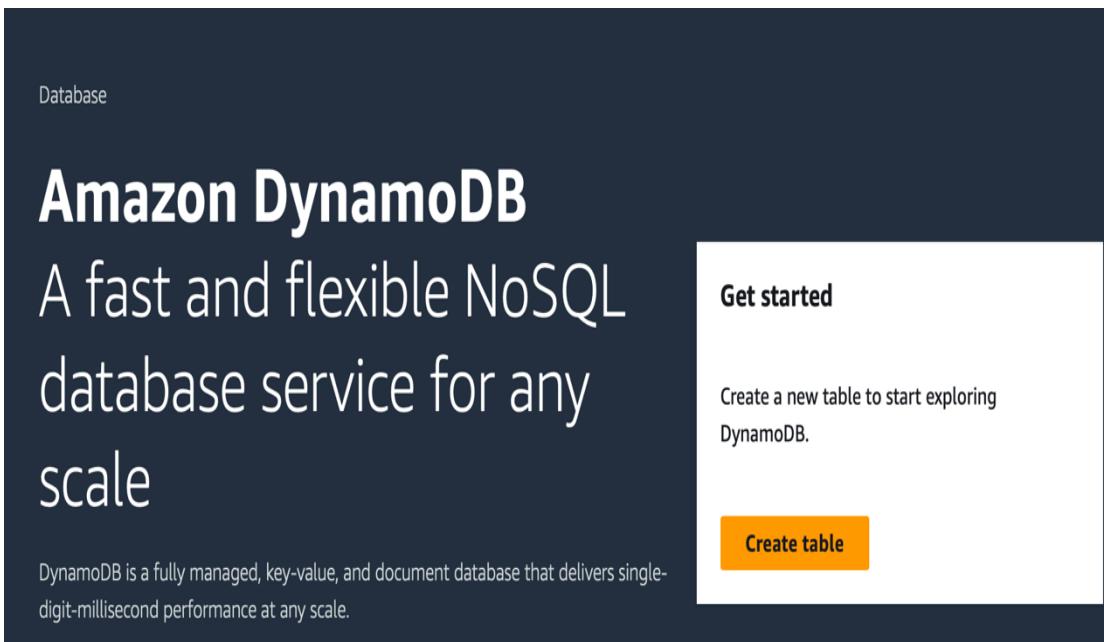


Figure 4.45. Deploy DynamoDB

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

DynamoDB > Tables > Create table

Create table

Table details Info

DynamoDB is a schemaless database that requires only a table name and a primary key when you create the table.

Table name
This will be used to identify your table.
 Between 3 and 255 characters, containing only letters, numbers, underscores (_), hyphens (-), and periods (.)

Partition key
The partition key is part of the table's primary key. It is a hash value that is used to retrieve items from your table and allocate data across hosts for scalability and availability.
 String ▾
1 to 255 characters and case sensitive.

Sort key - optional
You can use a sort key as the second part of a table's primary key. The sort key allows you to sort or search among all items sharing the same partition key.
 String ▾
1 to 255 characters and case sensitive.

Figure 4.46. Deploy DynamoDB

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

Tags

Tags are pairs of keys and optional values, that you can assign to AWS resources. You can use tags to control access to your resources or track your AWS spending.

No tags are associated with the resource.

Add new tag

You can add 50 more tags.

Create table

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.

The screenshot shows the AWS IAM Roles page. On the left, there's a sidebar with "Identity and Access Management (IAM)" at the top, followed by "Dashboard", "Access management" (with "User groups", "Users", and "Roles" listed), "Policies", "Identity providers", and "Account settings". Below that is "Access reports" and "Access Analyzer". The main area is titled "Roles (6) Info" and contains a table of existing roles:

Role name	Trusted entities	Last activity
AmazonSSMManagedCoreRole	AWS Service: ec2	12 days ago
AWSServiceRoleForApplicationAutoScaling_DynamoDBTable	AWS Service: dynamodb.application	15 minutes ago
AWSServiceRoleForOrganizations	AWS Service: organizations (Service-Linked Role)	-
AWSServiceRoleForSSO	AWS Service: sso (Service-Linked Role)	49 minutes ago
AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-

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

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

The screenshot shows the "Select trusted entity" configuration page. At the top, it says "Trusted entity type". There are five options: "AWS service" (selected, highlighted in blue), "AWS account", "Web identity", "SAML 2.0 federation", and "Custom trust policy". Below that, under "Use case", it says "Allow an AWS service like EC2, Lambda, or others to perform actions in this account." A dropdown menu for "Service or use case" shows "EC2" selected. The bottom right corner has a dropdown arrow.

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.

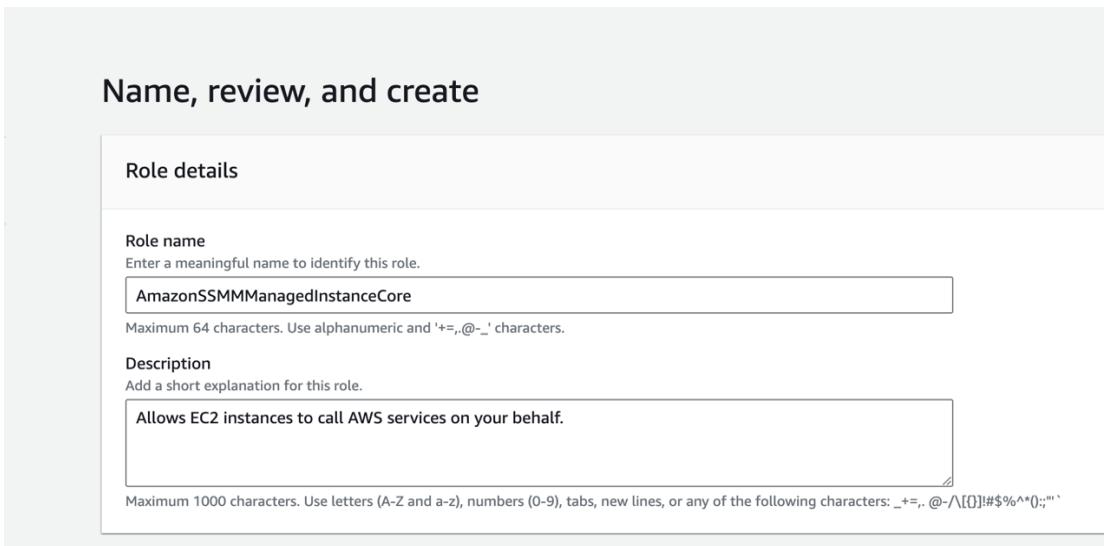


Figure 4.50. Create Role for EC2 to Access S3 and DynamoDB

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

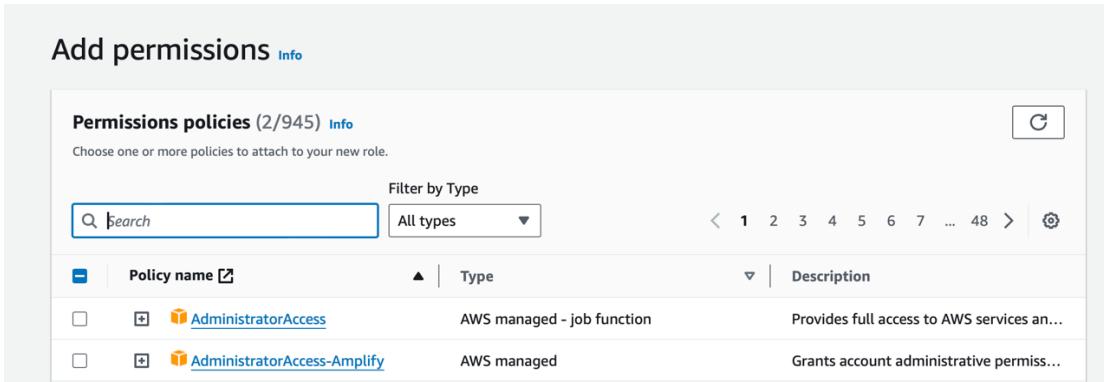


Figure 4.51. Create Role for EC2 to Access S3 and DynamoDB

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

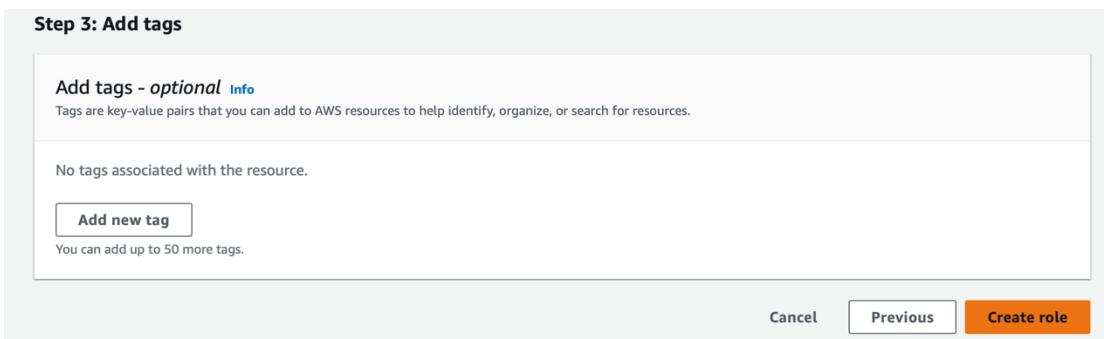


Figure 4.52. Create Role for EC2 to Access S3 and DynamoDB

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.

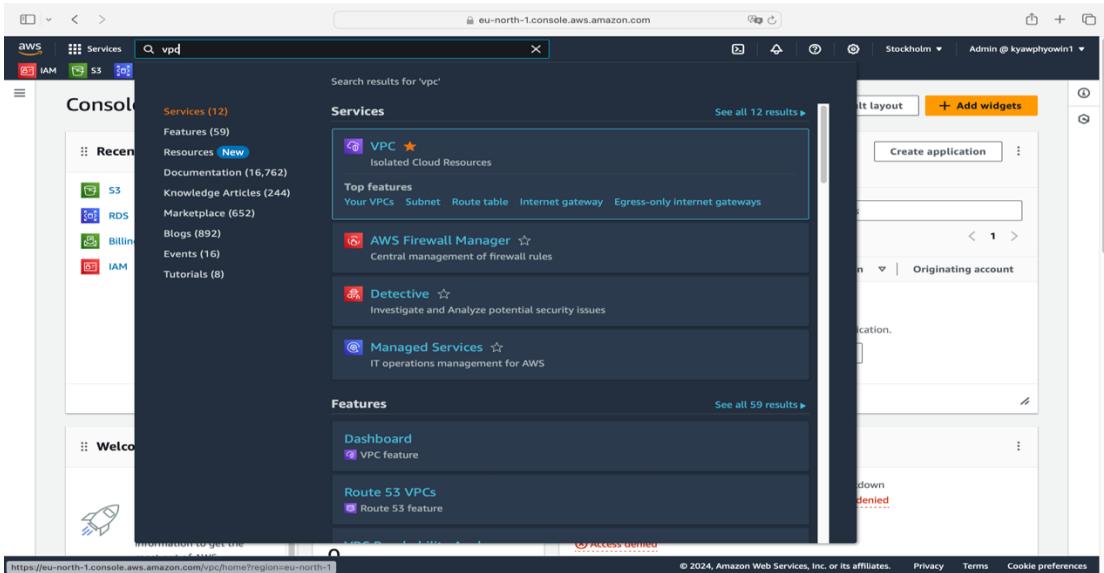


Figure 4.53. Creating VPC

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

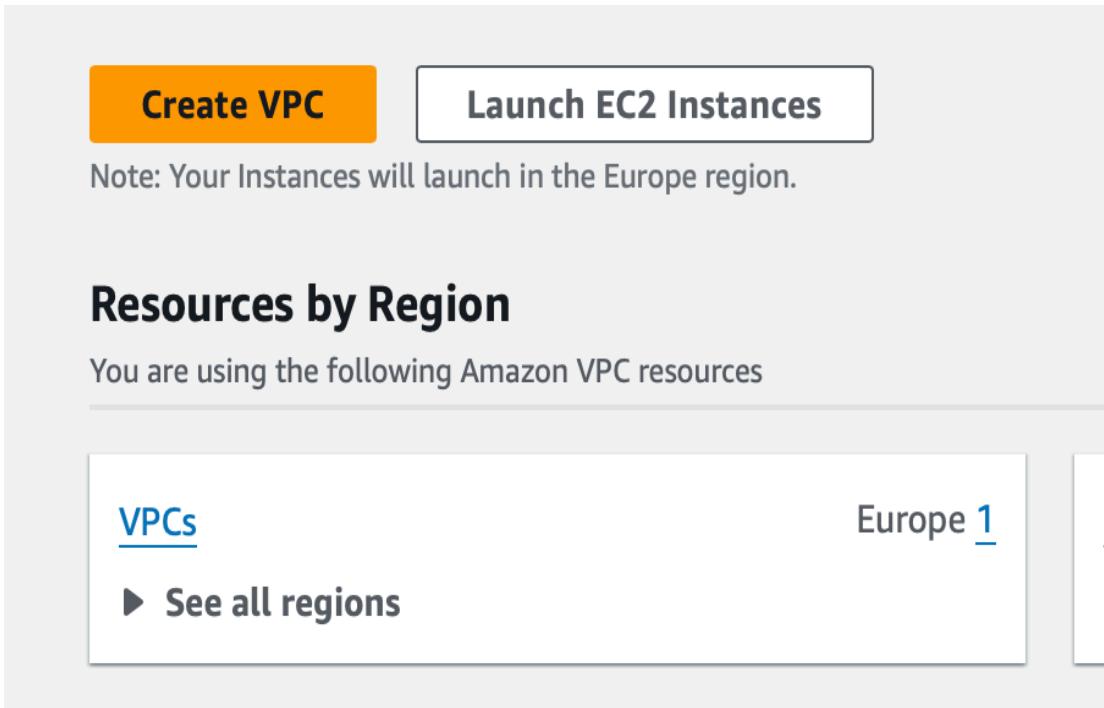


Figure 4.54. Creating VPC

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

VPC > Your VPCs > Create VPC

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings		<small>CreateVpc</small>
Resources to create <small>Info</small> Create only the VPC resource or the VPC and other networking resources.		
<input checked="" type="radio"/> VPC only <input type="radio"/> VPC and more		
Name tag - optional Creates a tag with a key of 'Name' and a value that you specify. <input type="text" value="my-vdc"/>		
IPv4 CIDR block <small>Info</small> <input checked="" type="radio"/> IPv4 CIDR manual input <input type="radio"/> IPAM-allocated IPv4 CIDR block		
IPv4 CIDR <input type="text" value="10.0.0.0/16"/> <small>CIDR block size must be between /16 and /28.</small>		
IPv6 CIDR block <small>Info</small> <input checked="" type="radio"/> No IPv6 CIDR block <input type="radio"/> IPAM-allocated IPv6 CIDR block <input type="radio"/> Amazon-provided IPv6 CIDR block <input type="radio"/> IPv6 CIDR owned by me		

Figure 4.55. Creating VPC

Figure 4.56 presented that VPC had created successfully.

You successfully created **vpc-0570d5a0809bc4bd7 / my-vdc**

VPC > Your VPCs > **vpc-0570d5a0809bc4bd7 / my-vdc**

Details <small>Info</small>			
VPC ID	vpc-0570d5a0809bc4bd7	State	Available
Tenancy	Default	DHCP option set	dopt-023c910b34993e6e8
Default VPC	No	IPv4 CIDR	10.0.0.0/16
Network Address Usage metrics	Disabled	Route 53 Resolver DNS Firewall rule groups	Owner ID 010526242997
			Main route table rtb-066eb6cefde3f40e5
			Main network ACL acl-03807a91b83a86a4b
			IPv6 CIDR (Network border group) -

Resource map Info

- VPC** Show details
Your AWS virtual network
my-vdc
- Subnets (0)**
Subnets within this VPC
- Route tables (1)**
Route network traffic to resources
rtb-066eb6cefde3f40e5

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.

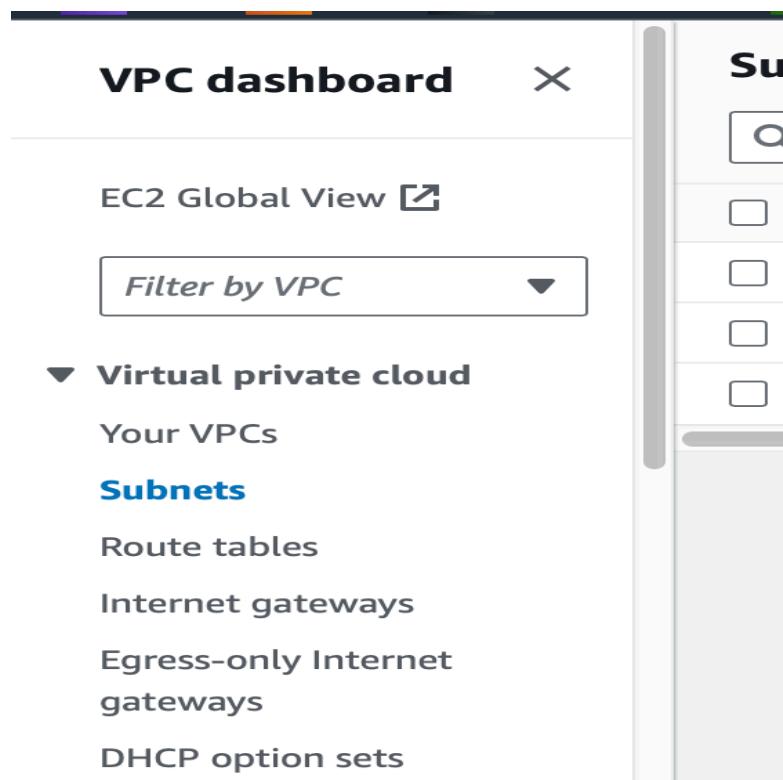


Figure 4.57. Set Up Network Configuration

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

The screenshot shows the "Create subnet" wizard. At the top, there's a breadcrumb navigation: "VPC > Subnets > Create subnet". Below it, there's a "CreateSubnet" button and a "Info" link. The main form is divided into sections:

- VPC**: Contains a "VPC ID" field with the value "vpc-0570d5a0809bc4bd7 (my-vdc)".
- Associated VPC CIDRs**: Contains an "IPv4 CIDRs" field with the value "10.0.0.0/16".
- Subnet settings**: A note says "Specify the CIDR blocks and Availability Zone for the subnet." It contains a "Subnet 1 of 1" section.
- Subnet 1 of 1**: Contains a "Subnet name" field with the value "my-subnet-01". A note below says "The name can be up to 256 characters long."

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.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
Europe (Stockholm) / eu-north-1a

IPv4 VPC CIDR block [Info](#)
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/16

IPv4 subnet CIDR block
10.0.0.1/24 CreateSubnet 256 IPs
< > ^ v

▼ Tags - optional
Key Value - optional
Name public1 Remove
Add new tag
You can add 49 more tags.
Remove
Add new subnet

Cancel **Create subnet**

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”.

Subnets (1/4) [Info](#)
Last updated about 3 hours ago

Name	Subnet ID	State	VPC
-	subnet-026f6470f08b8927a	Available	vpc-07018acbd28
-	subnet-0cdc86b9d2b474160	Available	vpc-07018acbd28
<input checked="" type="checkbox"/> public1	subnet-05f0e8e1ee5ca5623	Available	vpc-0570d5a0809
-	subnet-0bc4874b21b0125b5	Available	vpc-07018acbd28

Actions ▲ **Create subnet**
View details
Create flow log
Edit subnet settings
Edit IPv6 CIDR subnets
Edit network ACL association
Edit route table association
Edit CIDR reservations
Share subnet
Manage tags
Delete subnet

subnet-05f0e8e1ee5ca5623 / public1
Details Flow logs Route table Network ACL CIDR reservations Sharing Tags

Figure 4.60. Set Up Network Configuration

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

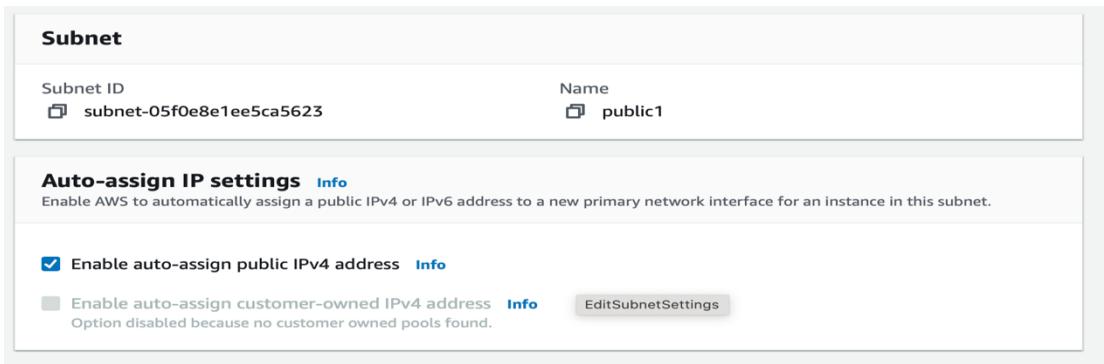


Figure 4.61. Set Up Network Configuration

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

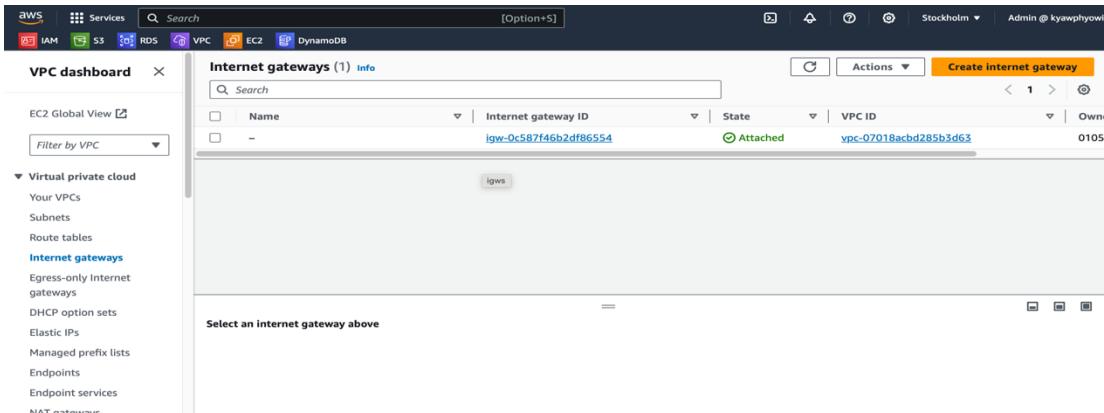


Figure 4.62. Set Up Network Configuration

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

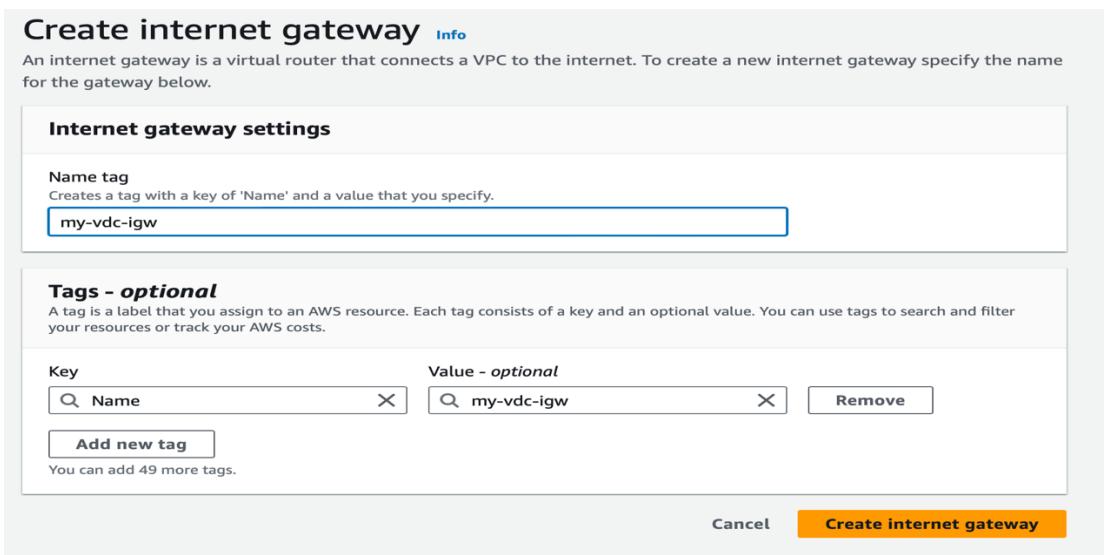


Figure 4.63. Set Up Network Configuration

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

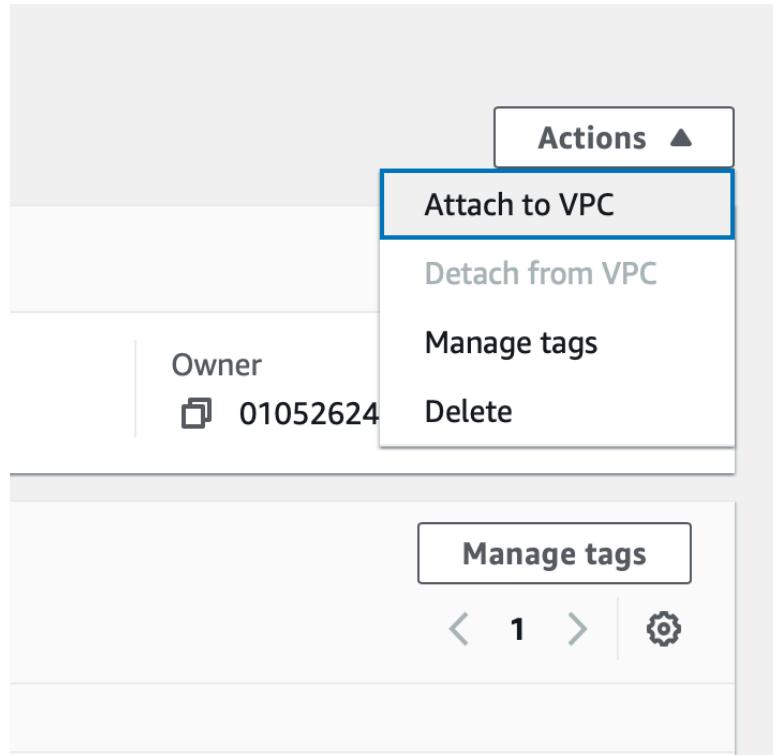


Figure 4.64. Set Up Network Configuration

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

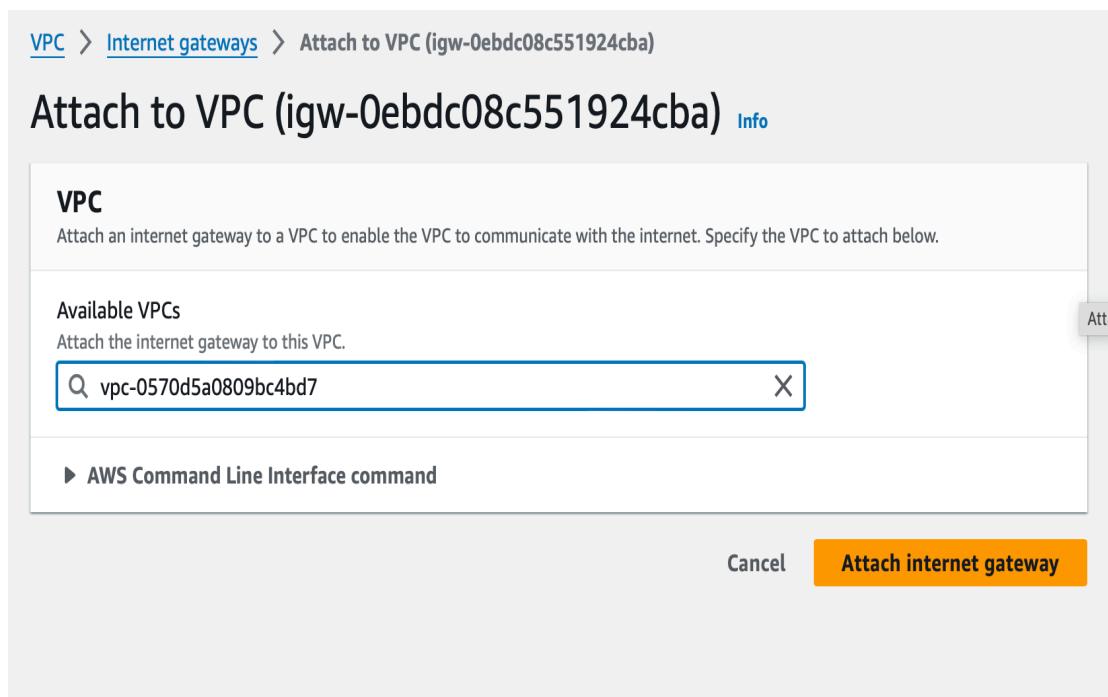


Figure 4.65. Set Up Network Configuration

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.

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-085864a19ddc5918	-	-	Yes
rtb-066eb6cefde3f40e5	Yes	-	Yes

Figure 4.66. Set Up Network Configuration

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

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

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.

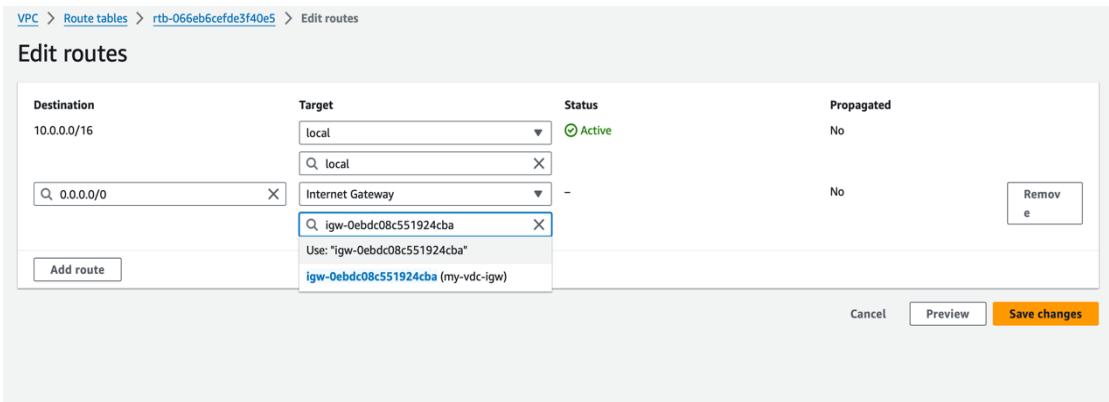


Figure 4.68. Set Up Network Configuration

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

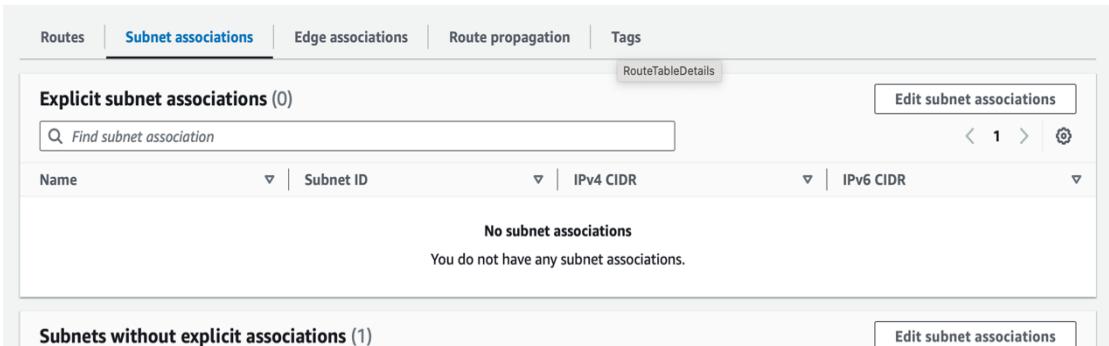


Figure 4.69. Set Up Network Configuration

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

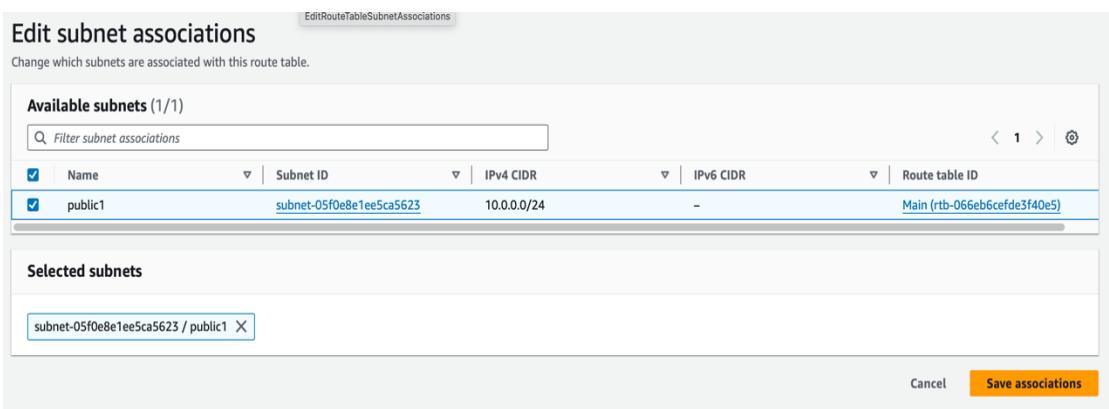


Figure 4.70. Set Up Network Configuration

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

The screenshot shows the AWS VPC Security Groups page. On the left, there's a sidebar with navigation links for Peering connections, Security (selected), Network ACLs, Security groups (selected), DNS firewall, Rule groups, Domain lists, and Network Firewall. The main area displays a table titled "Security Groups (2) Info". The table has columns for Name, Security group ID, Security group name, and VPC ID. Two rows are listed: one for "sg-0278848c5ae360d1f" and another for "sg-04fe184070be0d54c", both under the "default" security group and VPC ID "vpc-07018acd285b3d63". A "Create security group" button is located at the top right of the table area.

Figure 4.71. Set Up Network Configuration

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

The screenshot shows the "Create security group" wizard. The first step, "Basic details", is completed. The "Security group name" field contains "myvdcSG". The "Description" field contains "Allow HTTP access". The "VPC" dropdown is set to "vpc-0570d5a0809bc4bd7 (my-vdc)". Below the form, a note states: "A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below."

Figure 4.72. Set Up Network Configuration

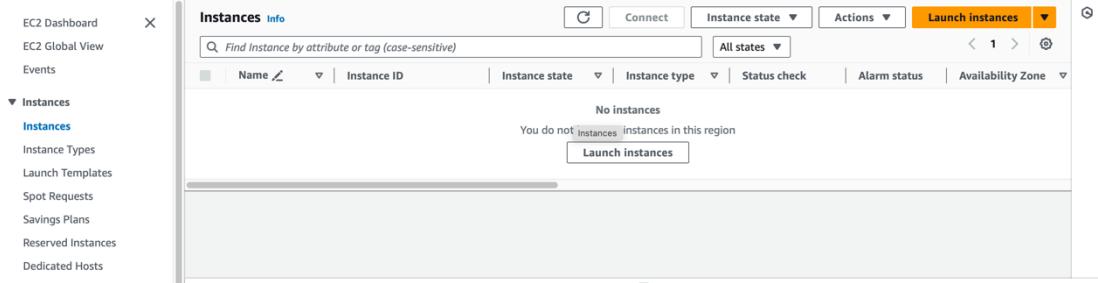
Click on “Add rule”, select the type of traffic “HTTP”, define where the traffic is allowed from (e.g. 0.0.0.0/0) and click on “Create security group” as shown in Figure 4.73.

The screenshot shows the "Create security group" wizard. The second step, "Outbound rules", is shown with two rules defined. The first rule is "All traffic" with "Type: All traffic", "Protocol: All", "Port range: All", and "Destination: Custom" (0.0.0.0/0). The second rule is "HTTP" with "Type: HTTP", "Protocol: TCP", "Port range: 80", and "Destination: Anywhere" (0.0.0.0/0). A warning message at the bottom of this section states: "⚠ Rules with destination of 0.0.0.0/0 or ::/0 allow your instances to send traffic to any IPv4 or IPv6 address. We recommend setting security group rules to be more restrictive and to only allow traffic to specific known IP addresses." The third step, "Tags - optional", shows no tags and an "Add new tag" button. The fourth step, "CreateSecurityGroup", shows the "Create security group" button highlighted.

Figure 4.73. Set Up Network Configuration

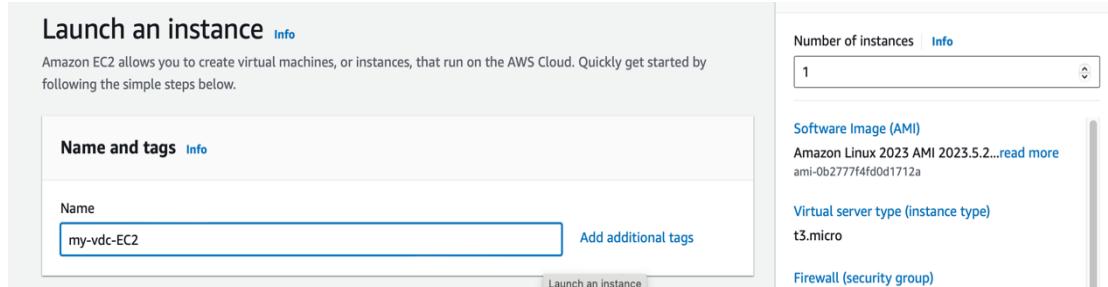
4.9. Step-By-Step Guide to Launch Elastic Compute Cloud (EC2)

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



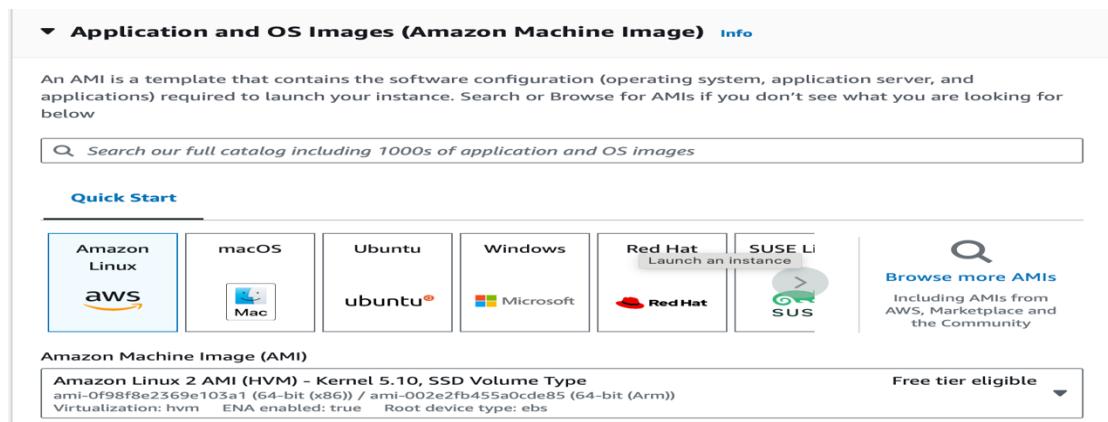
4.74. Launch EC2 Instance

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.

The screenshot shows the AWS EC2 instance creation wizard. At the top, it displays the selected architecture as "64-bit (x86)" and the AMI ID as "ami-0f98f8e2369e103a1". A "Verified provider" badge is present. Below this, the "Instance type" section shows the "t3.micro" instance type, which is "Free tier eligible". It provides detailed pricing information for various On-Demand and Reserved instances across different operating systems. The "Key pair (login)" section indicates that no key pair is selected, with a note that you can use a key pair to securely connect to your instance. The "Configure storage" section shows a root volume of 8 GiB using the gp2 storage type. A message informs free-tier eligible customers about EBS storage options. The "Network settings" section is partially visible at the bottom.

4.77. Launch EC2 Instance

As demonstrated in Figure 4.78 configure storage as your needs.

This screenshot shows the "Configure storage" step of the EC2 instance creation wizard. It specifies a root volume of 8 GiB using the gp2 storage type. A message box informs users that free-tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. There is also a link to "Add new volume". Below this, there is a note about refresh backup information and Data Lifecycle Manager policies. The "File systems" section is shown with an "Edit" button.

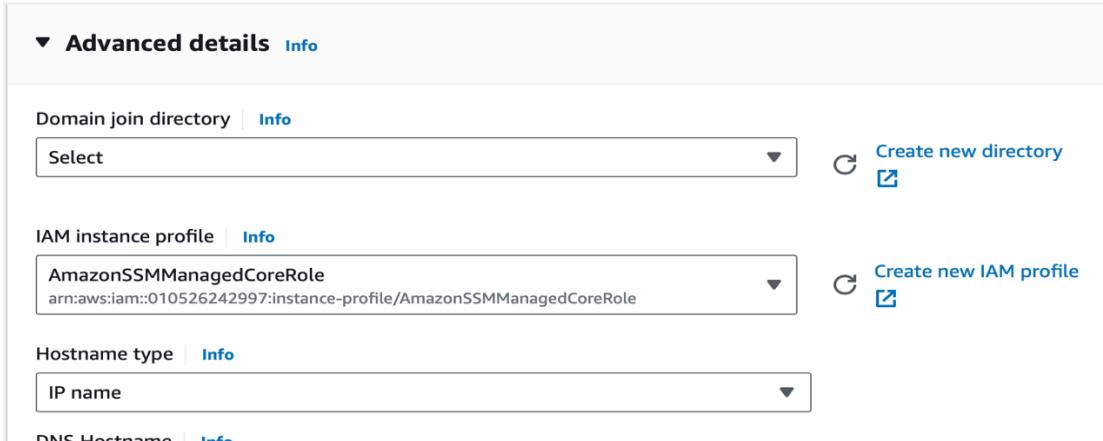
4.78. Launch EC2 Instance

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.

This screenshot shows the "Network settings" step of the EC2 instance creation wizard. It starts with a "VPC - required" section where "my-vdc" is selected. Below this, the "Subnet" section shows "public1" as the subnet, with details like VPC ID, owner, availability zone, and CIDR. A "Create new subnet" link is available. The "Auto-assign public IP" section has "Enable" selected. The "Firewall (security groups)" section allows adding rules to control traffic. It includes options to "Create security group" or "Select existing security group". The "Common security groups" section lists "myvdcSG" as the selected group. A note states that security groups added here will be added to all network interfaces. The "Advanced network configuration" section is partially visible at the bottom.

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.



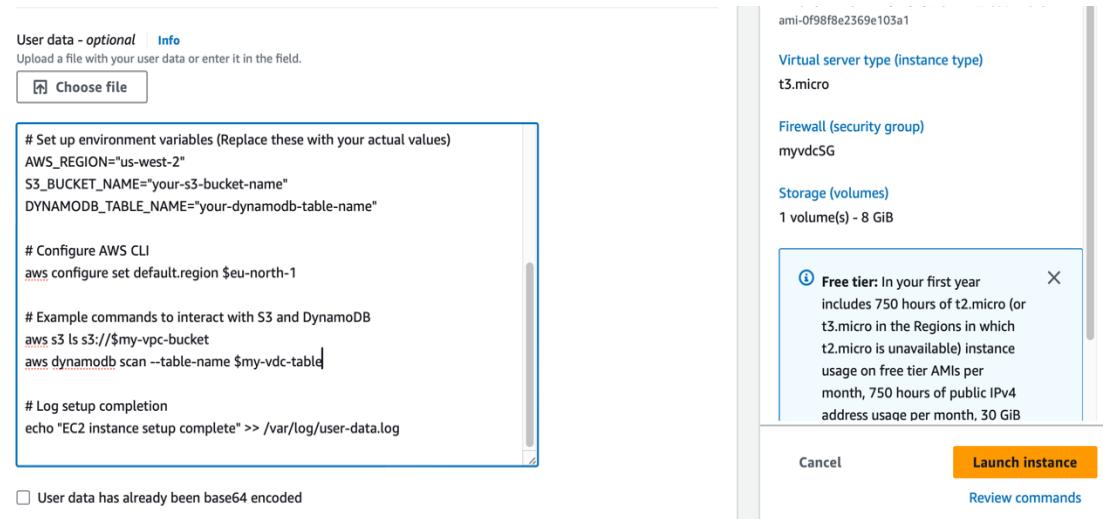
4.80. Launch EC2 Instance

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.

Instances (2) Info		C	Connect	Instance state ▼	Actions ▼	Launch instances ▼	
		<input type="text"/> Find Instance by attribute or tag (case-sensitive)		All states ▼			
		Instance state = running X	Clear filters				
	Name ▼	Instance ID	Instance state ▼	Instance type ▼	Status check	Alarm status	Availability Zone ▼
<input type="checkbox"/>	my-vdc-ec2	i-0d92d90145b2f0765	Running Q Q	t2.micro	2/2 checks passed View alarms +	us-east-1a	
<input type="checkbox"/>	myweb	i-0bc3ebc892179c365	Running Q Q	t2.micro	2/2 checks passed View alarms +	us-east-1a	

Figure 4.83. Launch EC2 Instance

4.10. Creating an Datadog account and Sign Up

Visit “datadoghq.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.

Get Started with Datadog

No credit card required
Try it free for 14 days and monitor as many servers as you like.
*Required Fields

Region*
Please choose carefully. You can't migrate data between regions.
Where do you want your data housed?

Europe (EU1)

Business Email*

Full Name*

Company*

Password*
Use at least 8 characters containing at least 1 number and 1 lowercase letter

Phone

*Required fields. By signing up, you agree to the [Master Subscription Agreement](#), [Privacy Policy](#), and [Cookie Policy](#).

Figure 4.85. Sign Up Datadog Monitoring Framework

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

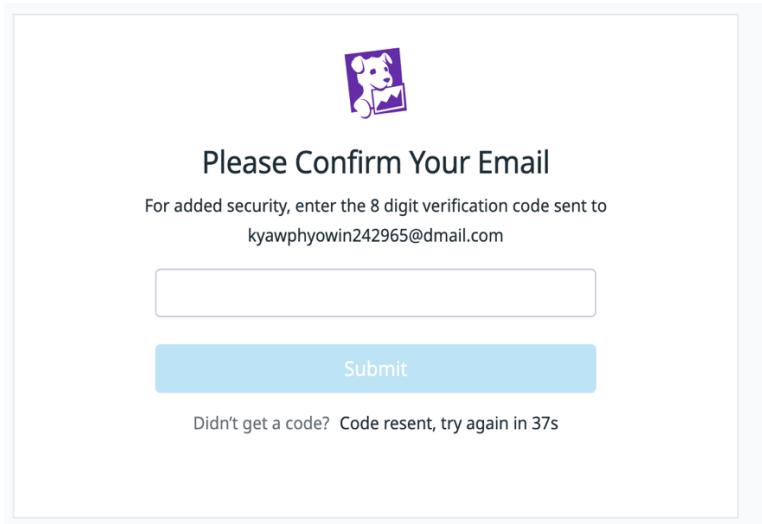


Figure 4.86. Sign Up Datadog Monitoring Framework

4.11. Integrate Datadog with AWS

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

1. Your Account **2. Your Stack** 3. Agent Setup

Tell us about your stack

Which services or software do you use? (optional)

Figure 4.87. Integrate Datadog with AWS

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

You haven't installed any Agents yet. Let's do it now!

Install or Update to the latest Agent version on Amazon Linux

The Datadog Agent has `x86_64` and `arm64` (ARM v8) packages. For other architectures, use the [source install](#).

Run this command to install or update...

```
DD_API_KEY=[REDACTED] DD_SITE="datadoghq.eu" bash -c "$(curl -L https://install.datadoghq.com/scripts/install_script_agent7.sh)"
```

- This will install the YUM packages for the Datadog Agent and will prompt you for your password.
- If the Agent is not already installed on your machine and you don't want it to start automatically after the installation, just prepend `DD_INSTALL_ONLY=true` to the above script before running it.
- If you have an existing agent configuration file, those values will be retained during the update.
- Otherwise, you can configure some of the agent options during the initial install process. For more information check the [install_script configuration options](#).

(For Amazon Linux 2022 installations on Agent version <= 7.39) The Agent requires the `libcrypt-compat` package:

```
dnf install -y libcrypt-compat
```

> Manual Step by Step Instructions

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)"`”.

```
mac — ec2-user@ip-10-0-0-37:~ — curl -sSfL https://install.datadoghq.com/scripts/install_script.sh | bash
AL2 End of Life is 2025-06-30.
A newer version of Amazon Linux is available!
Amazon Linux 2023, GA and supported until 2028-03-15.
https://aws.amazon.com/linux/amazon-linux-2023/
-bash: warning: setlocale: LC_CTYPE: cannot change locale (UTF-8): No such file or directory
[ec2-user@ip-10-0-0-37 ~]$ Connection to 54.92.130.63 closed by remote host.
Connection to 54.92.130.63 closed.
[mac0Kyaw-Physos-Mac ~ % DD_API_KEY=1769e101c4d8a08cc5549331c0961953 DD_SITE="datadoghq.eu" bash -c "$(curl -L https://install.datadoghq.com/scripts/install_mac_os.sh)"
% Total    % Received % Xferd  Average Speed   Time   Time     Current
          Dload  Upload Total Spent   Spent    Left  Speed
100 19506  100 19506    0      0  23561      0 --:--:-- --:--:-- 23557
Warning: DD_AGENT_MAJOR_VERSION not set. Installing Agent version 7 by default.
* Downloading datadog-agent
[Password:
Sorry, try again.
[Password:
#####
[ 22.3%
```

Figure 4.89. Integrate Datadog with AWS

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

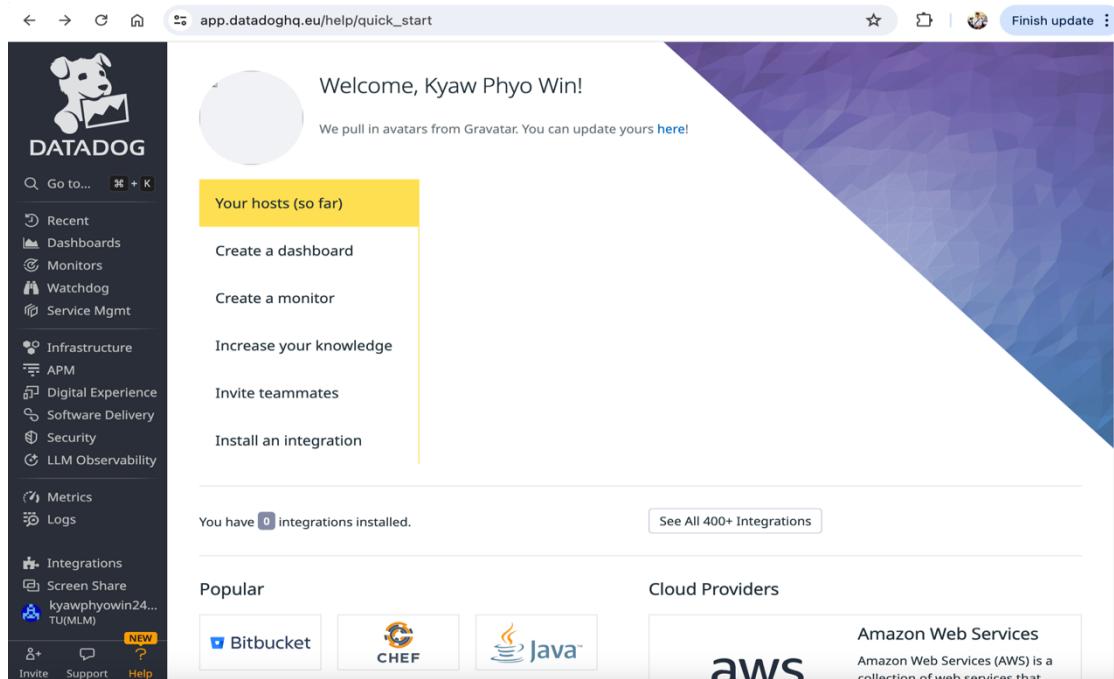


Figure 4.90. Integrate Datadog with AWS

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

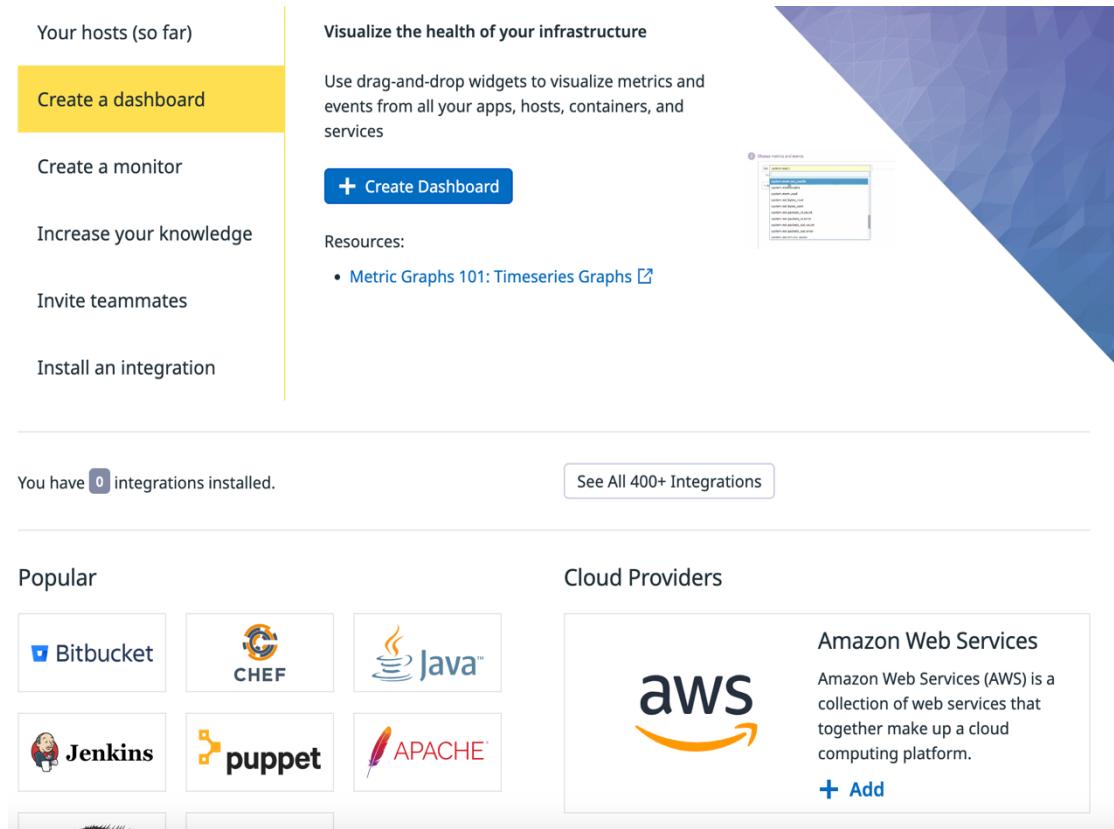


Figure 4.91. Integrate Datadog with AWS

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

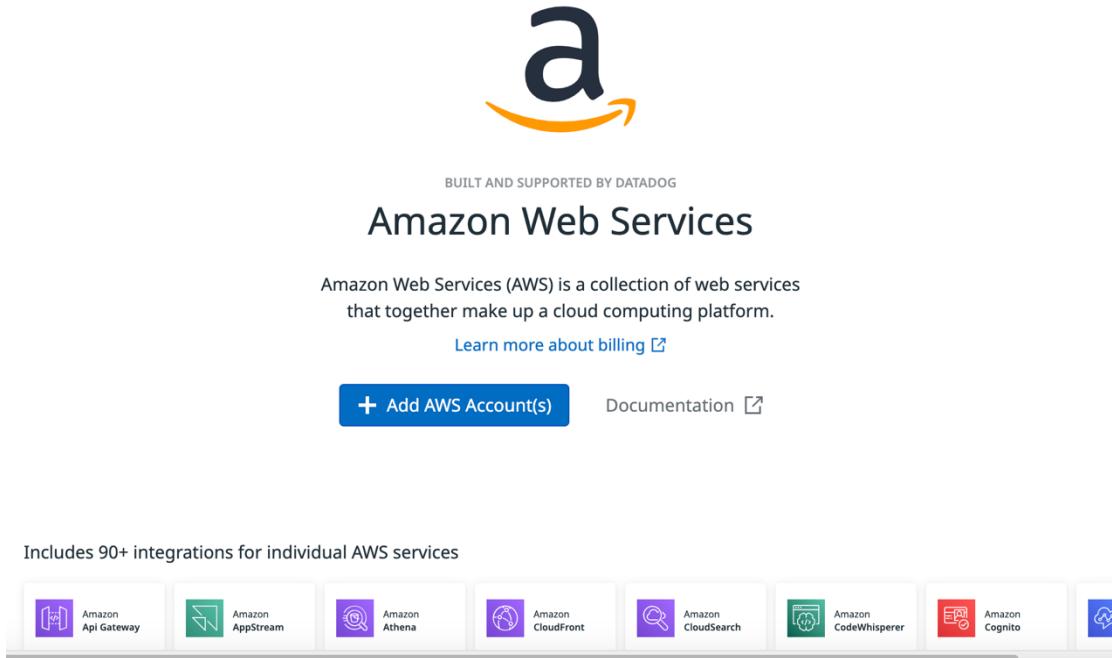


Figure 4.92. Integrate Datadog with AWS

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

[Integrations > Amazon Web Services > Add New AWS Account\(s\)](#)

Add New AWS Account(s)

[Add a Single AWS Account](#)

[Add Multiple AWS Accounts](#)

Choose a method for adding your AWS account:

Automatically using CloudFormation RECOMMENDED

Use a CloudFormation template to create a stack that automatically adds the IAM permissions and other resources necessary for integrating your AWS account.

Manually

Add the IAM permissions needed to integrate your AWS account in the AWS console, then finish setup in Datadog.

1 Select Access Type

Select between Role Delegation or Access Keys.

[Role Delegation ▾](#)

2 Add Permissions in AWS

Copy the External ID [?](#) then follow our documentation for creating the necessary IAM resources in the AWS console.

AWS External ID: d2641bbdc2c1419090195d3a4d8d0802 [Copy](#) [Generate New ID](#)

Create the necessary IAM resources in the AWS Console.

[View Documentation](#)

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.

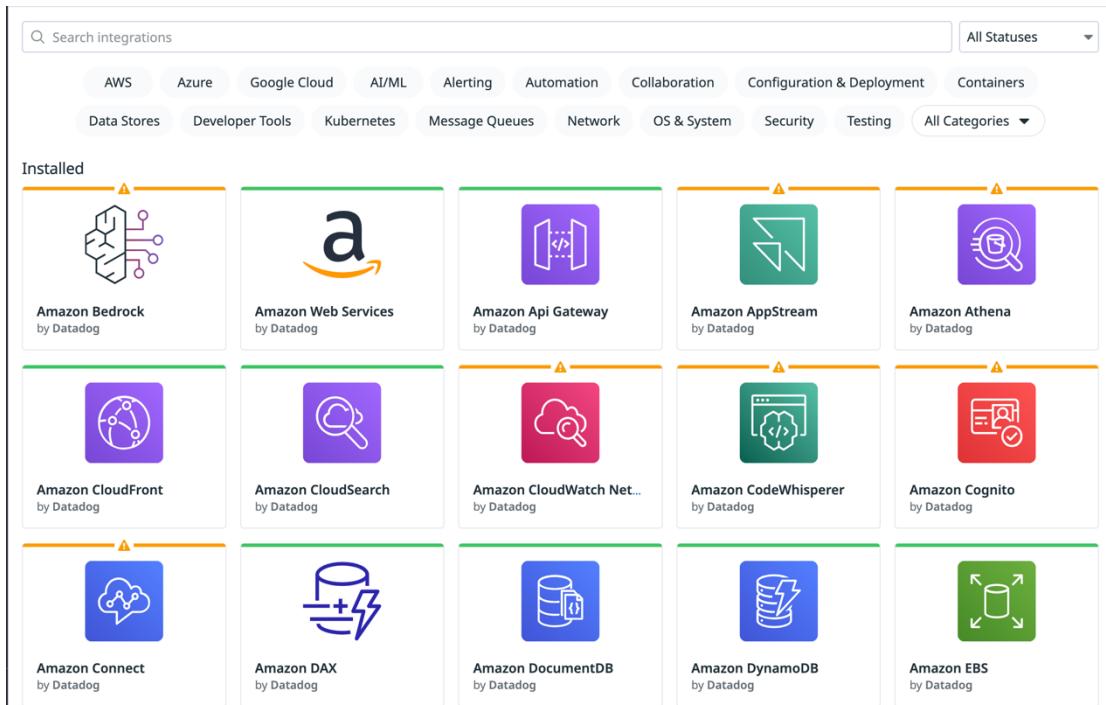


Figure 4.94. Integrate Datadog with AWS

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.

The screenshot shows the AWS S3 console. On the left, there's a sidebar with navigation links: Buckets, Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Block Public Access settings for this account, Storage Lens, Dashboards, Storage Lens groups, and AWS Organizations settings. The main area is titled "Amazon S3" and shows an "Account snapshot - updated every 24 hours" with a link to "All AWS Regions". There's also a "View Storage Lens dashboard" button. Below this, there are tabs for "General purpose buckets" (which is selected) and "Directory buckets". A sub-section titled "General purpose buckets (1)" shows a table with one item:

Name	AWS Region	IAM Access Analyzer	Creation date
my-vdc-s3	US East (N. Virginia) us-east-1	View analyzer for us-east-1	August 10, 2024, 15:48:01 (UTC+06:30)

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.

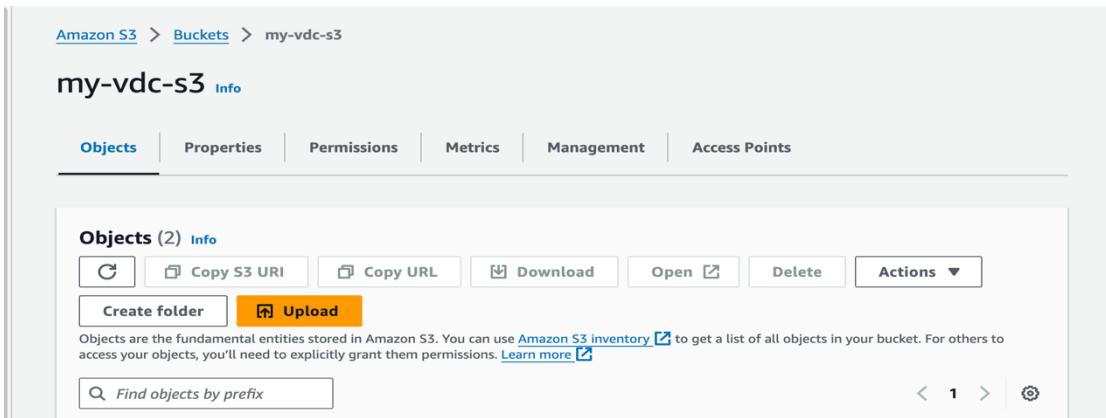


Figure 4.96. Testing and Validation

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.

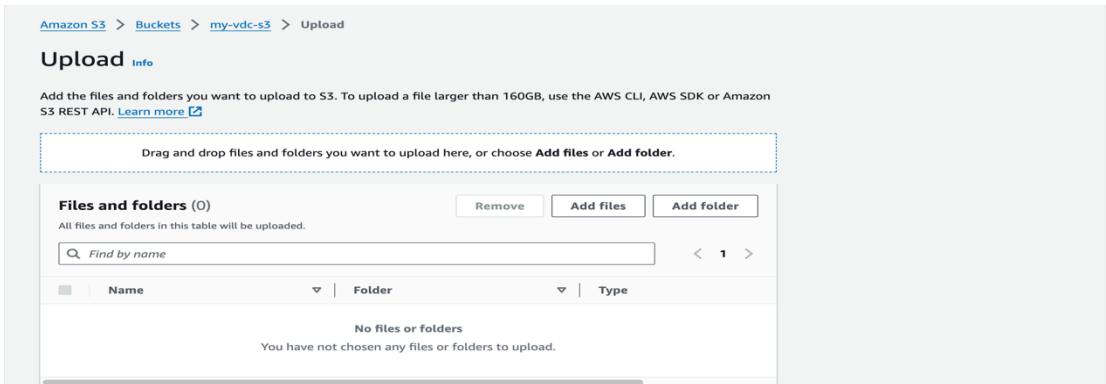


Figure 4.97. Testing and Validation

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

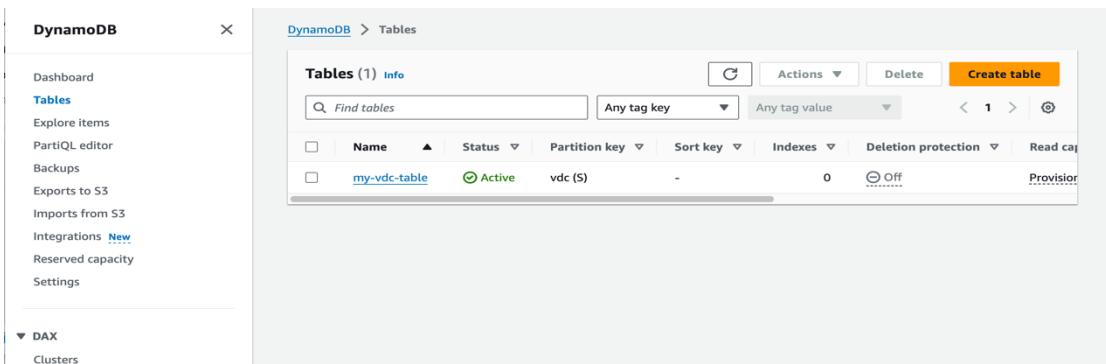


Figure 4.98. Testing and Validation

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

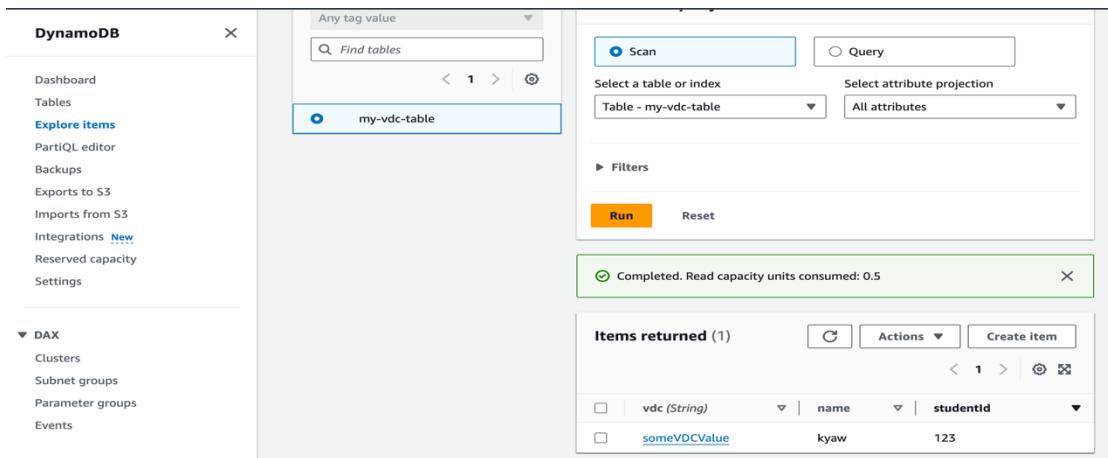


Figure 4.99. Testing and Validation

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

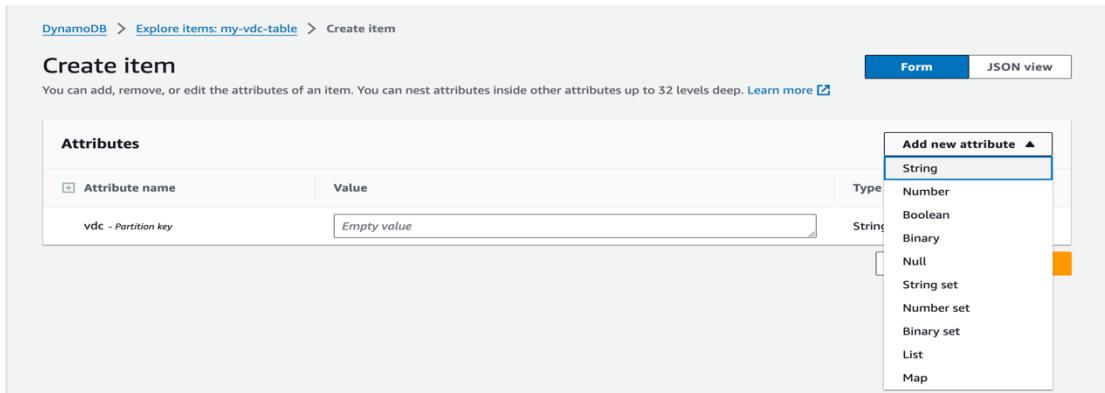


Figure 4.100. Testing and Validation

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.

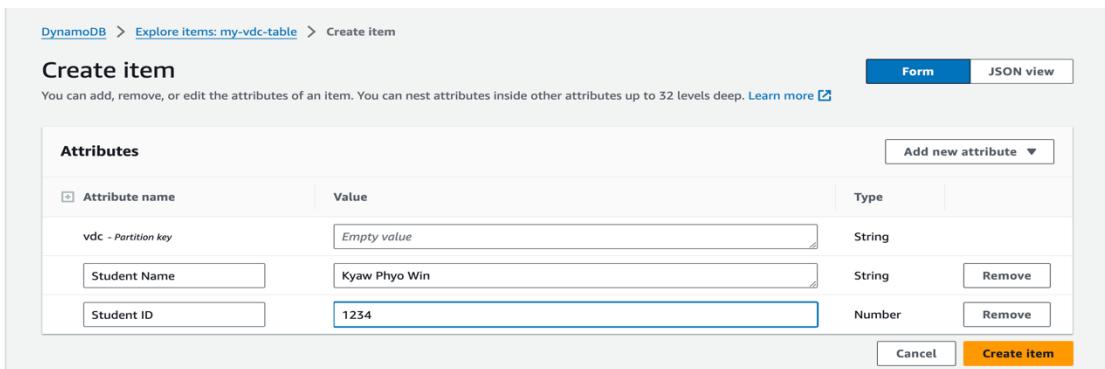
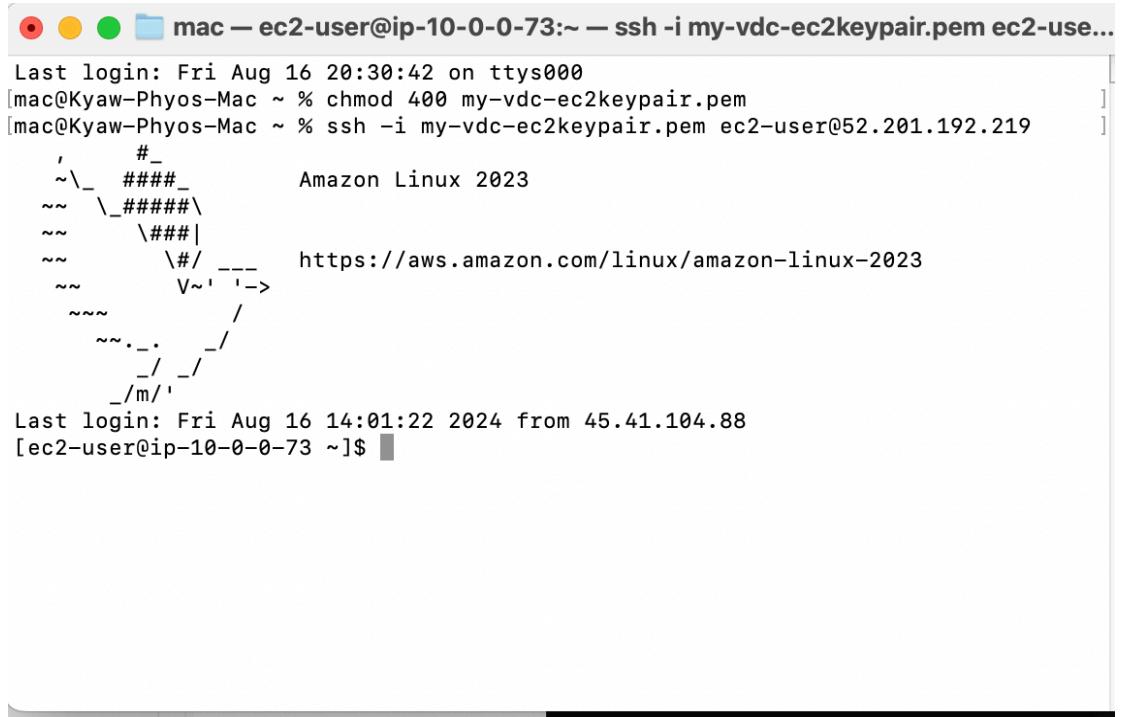


Figure 4.101. Testing and Validation

There are several methods to upload web files to EC2. Figure 4.102 presents step by step guide to add files to EC2 from 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.



```
Last login: Fri Aug 16 20:30:42 on ttys000
[mac@Kyaw-Phyos-Mac ~ % chmod 400 my-vdc-ec2keypair.pem
[mac@Kyaw-Phyos-Mac ~ % ssh -i my-vdc-ec2keypair.pem ec2-user@52.201.192.219
'      #
~\_ #####_      Amazon Linux 2023
~~ \#####\
~~ \###|
~~ \#/ ___ https://aws.amazon.com/linux/amazon-linux-2023
~~ \~' '-->
~~~ /
~~-. /-
/_m/
Last login: Fri Aug 16 14:01:22 2024 from 45.41.104.88
[ec2-user@ip-10-0-0-73 ~]$
```

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 command as shown in Figure 4.103.

For Amazon Linux or CentOS/RHEL:

```
bash
Copy code

sudo yum update -y
```

For Ubuntu/Debian:

```
bash
Copy code

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 Copy code
      sudo yum install git -y
```

For Ubuntu/Debian:

```
bash Copy code
      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 Copy code
      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 Copy code
      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 Copy code
      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                                     Copy code

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

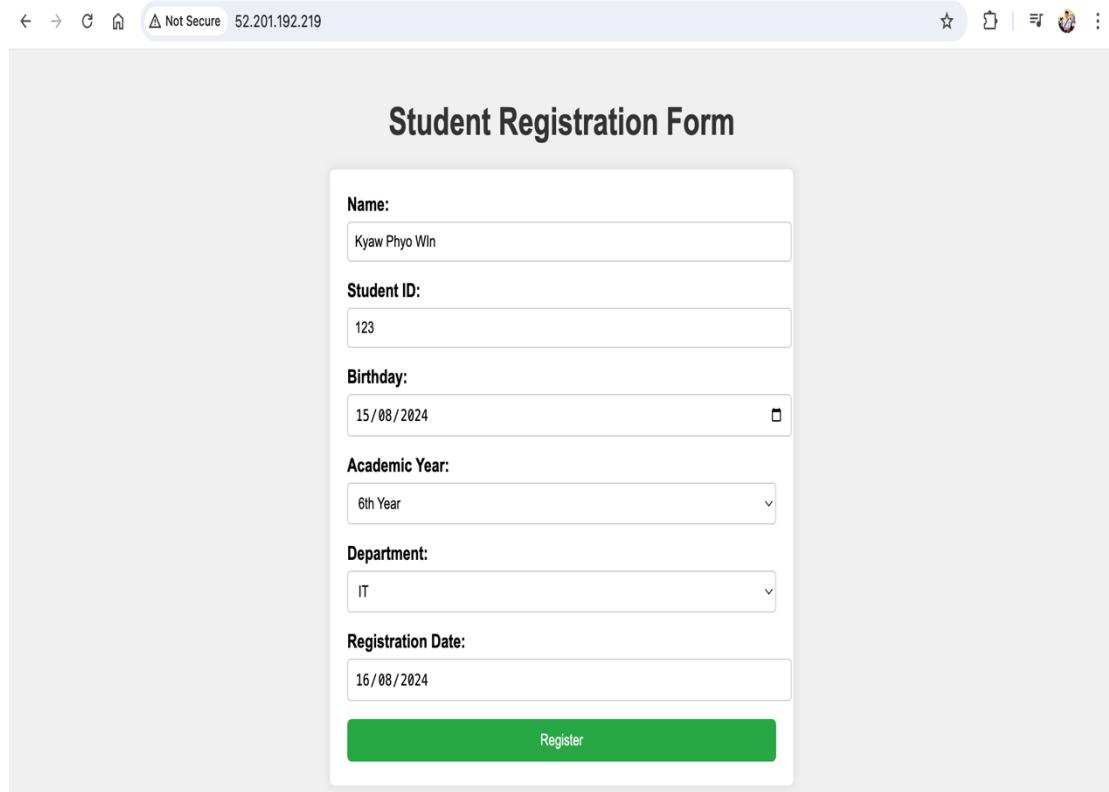
After installing dependencies, can typically start application using commands specific to technology stack as shown in Figure 4.109.

```
bash                                     Copy code

npm start
```

Figure 4.109. Testing and Validation

Figure 4.110 demonstrates example web page running on EC2.



The screenshot shows a web browser window with the URL `52.201.192.219`. The page title is "Student Registration Form". The form contains the following fields:

- Name:** Kyaw Phyto Wln
- Student ID:** 123
- Birthday:** 15/08/2024
- Academic Year:** 6th Year
- Department:** IT
- Registration Date:** 16/08/2024

A green "Register" button is at the bottom of the form.

Figure 4.110. Testing and Validation

Figure 4.111 presents monitoring dashboard for EC2.

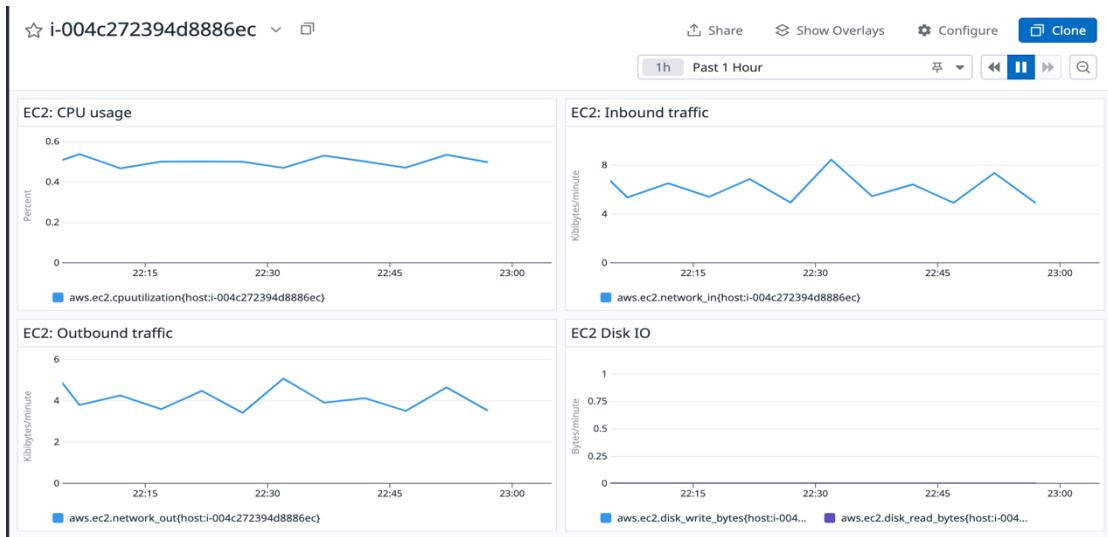


Figure 4.111. Testing and Validation

Figure 4.112 presents monitoring dashboard for EC2.

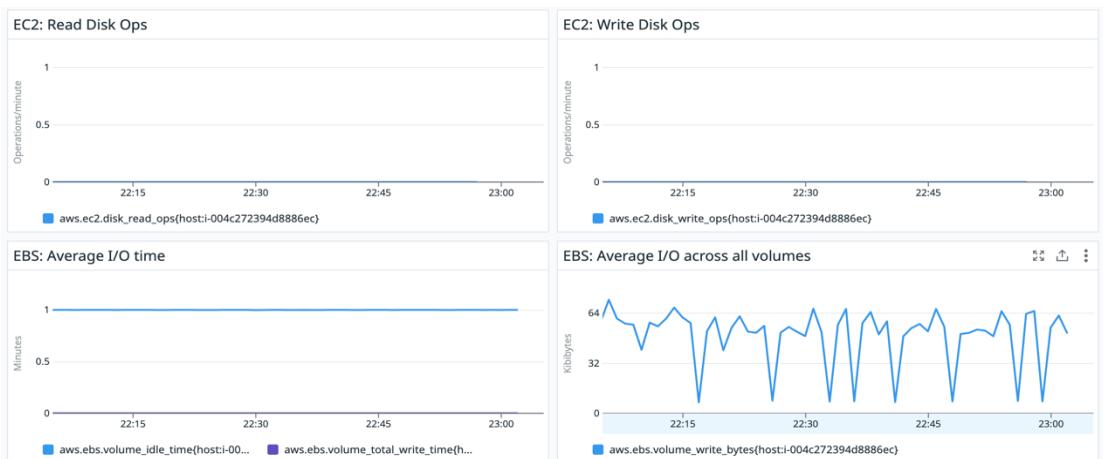


Figure 4.112. Testing and Validation

Figure 4.113 presents monitoring dashboard for EC2.

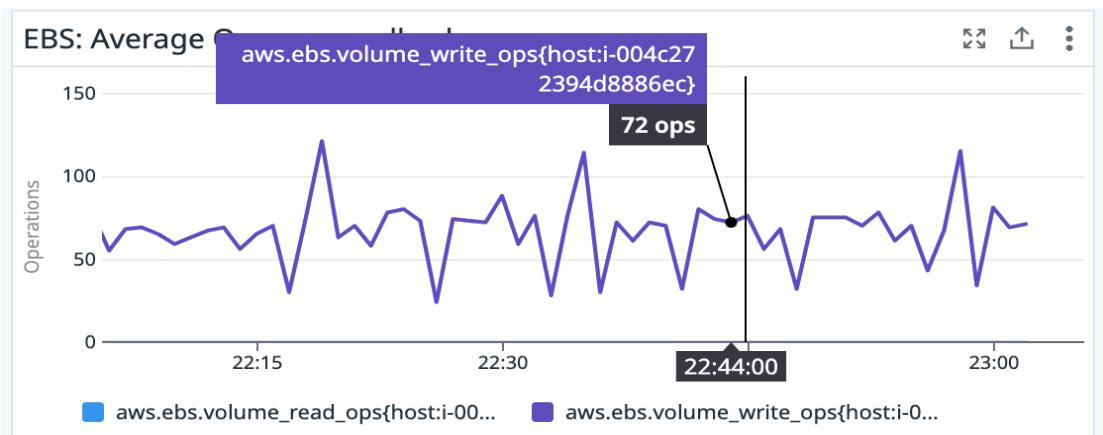


Figure 4.113. Testing and Validation