PRACTICAL -1

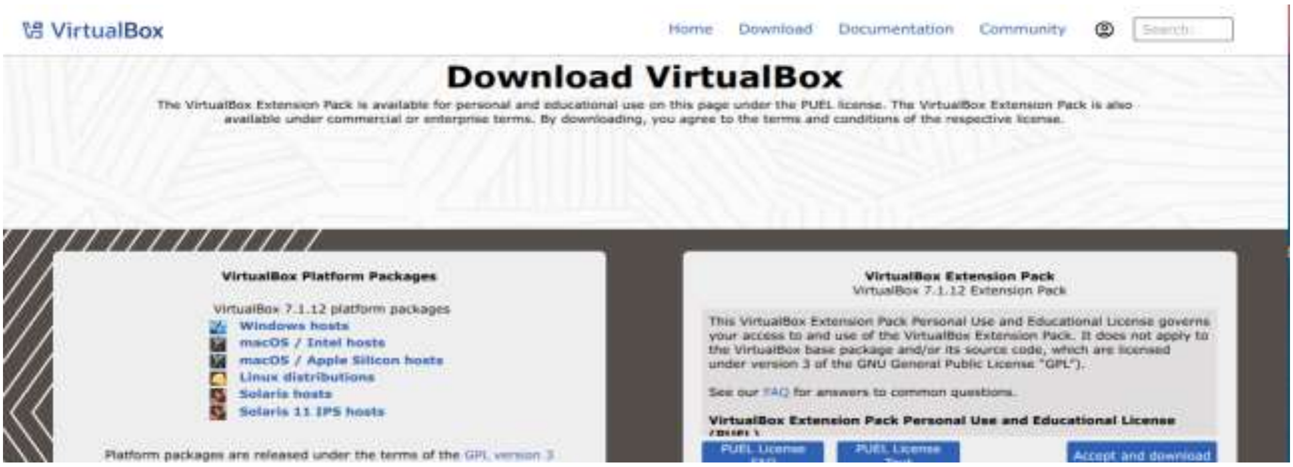
Aim: Installation of VirtualBox.

Introduction:

VirtualBox is a powerful open-source virtualization tool that allows users to run multiple operating systems on a single physical machine. It is commonly used for testing, development, and learning purposes without affecting the host system.

Procedure:

1. Visit the following link:
https://www.virtualbox.org/wiki/Downloads



Download VirtualBox

The VirtualBox Extension Pack is available for personal and educational use on this page under the PUEL license. The VirtualBox Extension Pack is also available under commercial or enterprise terms. By downloading, you agree to the terms and conditions of the respective license.

VirtualBox Platform Packages

VirtualBox 7.1.12 platform packages

- Windows hosts
- macOS / Intel hosts
- macOS / Apple Silicon hosts
- Linux distributions
- Solaris hosts
- Solaris 11 IPS hosts

Platform packages are released under the terms of the GPL version 3

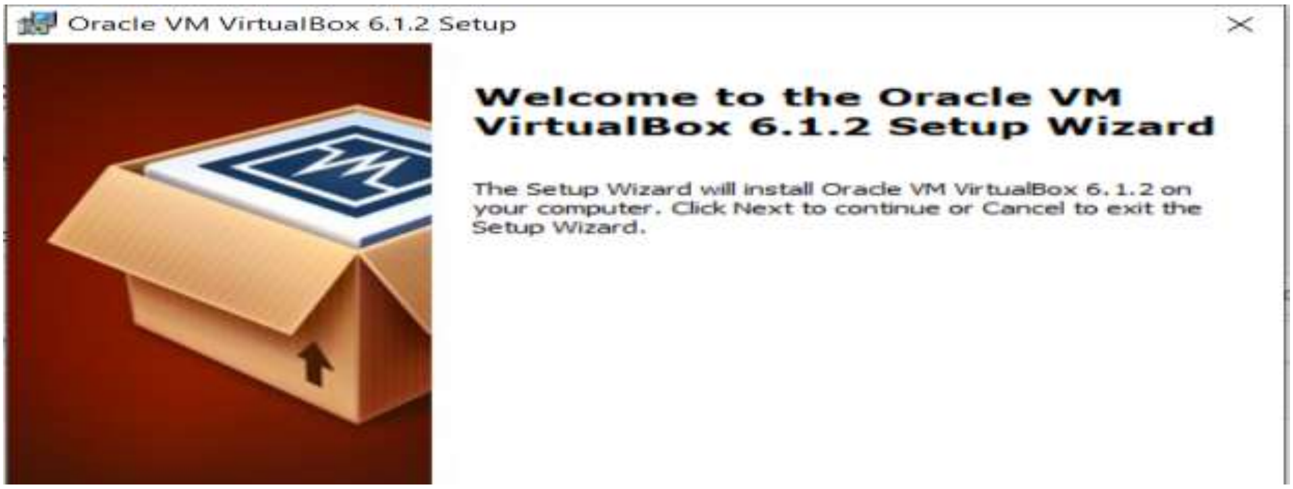
VirtualBox Extension Pack
VirtualBox 7.1.12 Extension Pack

This VirtualBox Extension Pack Personal Use and Educational License governs your access to and use of the VirtualBox Extension Pack. It does not apply to the VirtualBox base package and/or its source code, which are licensed under version 3 of the GNU General Public License "GPL").

See our FAQ for answers to common questions.

VirtualBox Extension Pack Personal Use and Educational License (PUEL)

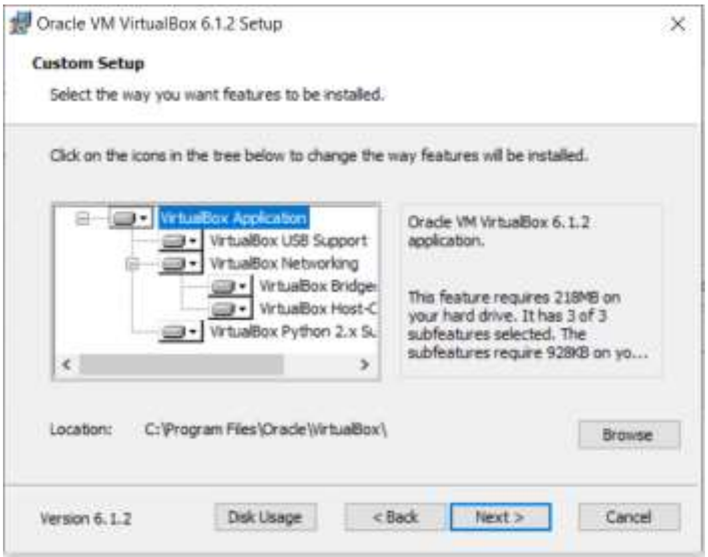
2. Download the appropriate host package for your operating system by clicking on ‘Windows hosts’, ‘macOS’ hosts, or ‘Linux distributions’.
3. Open the installer.



Welcome to the Oracle VM VirtualBox 6.1.2 Setup Wizard

The Setup Wizard will install Oracle VM VirtualBox 6.1.2 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

4. Leave the defaults in the installer and click on next.



Oracle VM VirtualBox 6.1.2 Setup

Custom Setup

Select the way you want features to be installed.

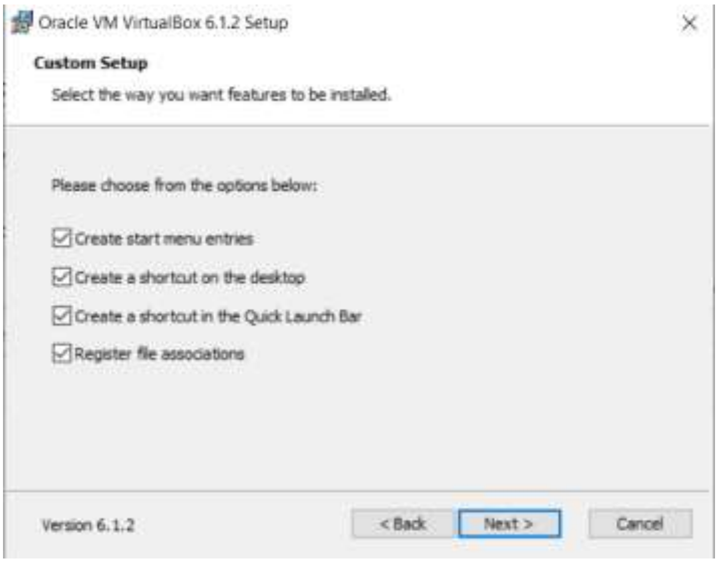
Click on the icons in the tree below to change the way features will be installed.

Oracle VM VirtualBox 6.1.2 application.

This feature requires 218MB on your hard drive. It has 3 of 3 subfeatures selected. The subfeatures require 928KB on yo...

Location: C:\Program Files\Oracle\VirtualBox\

Version 6.1.2



Oracle VM VirtualBox 6.1.2 Setup

Custom Setup

Select the way you want features to be installed.

Please choose from the options below:

☑ Create start menu entries

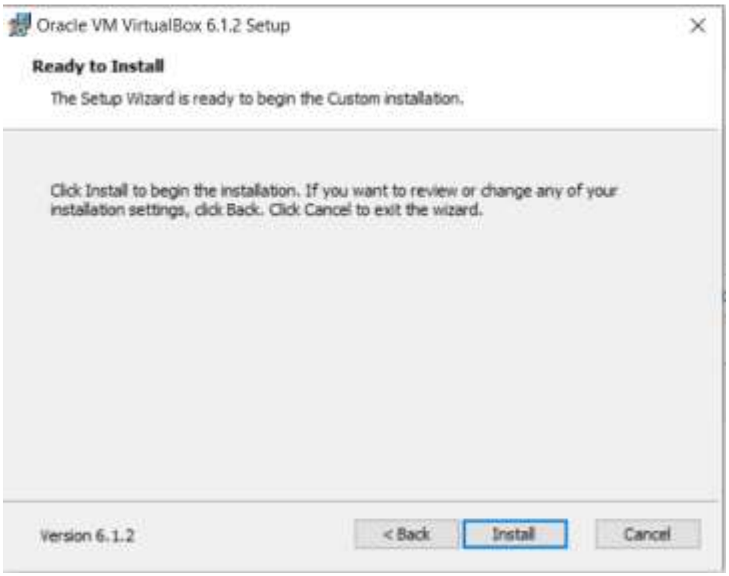
☑ Create a shortcut on the desktop

☑ Create a shortcut in the Quick Launch Bar

☑ Register file associations

Version 6.1.2

4. Click on 'Install'.



Oracle VM VirtualBox 6.1.2 Setup

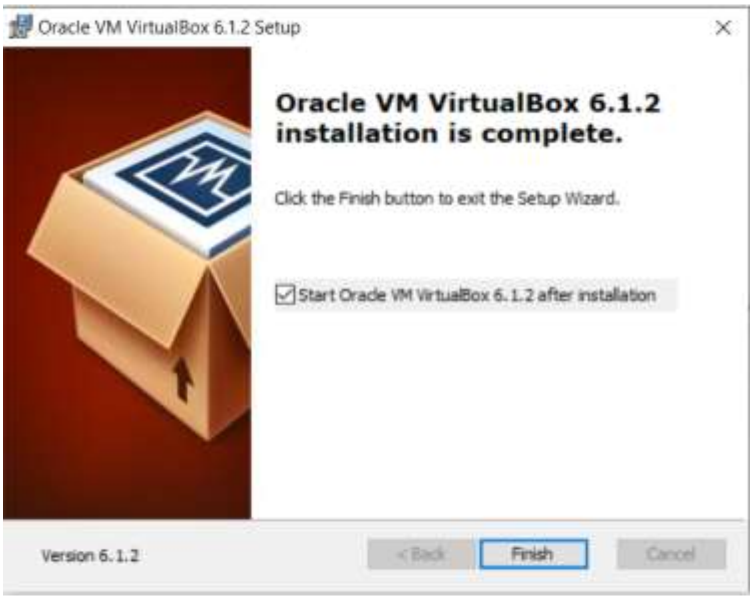
Ready to Install

The Setup Wizard is ready to begin the Custom installation.

Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Version 6.1.2

5. Click on ‘Install’ certificates if prompted.
6. Upon successful installation, you would see the screen like this:

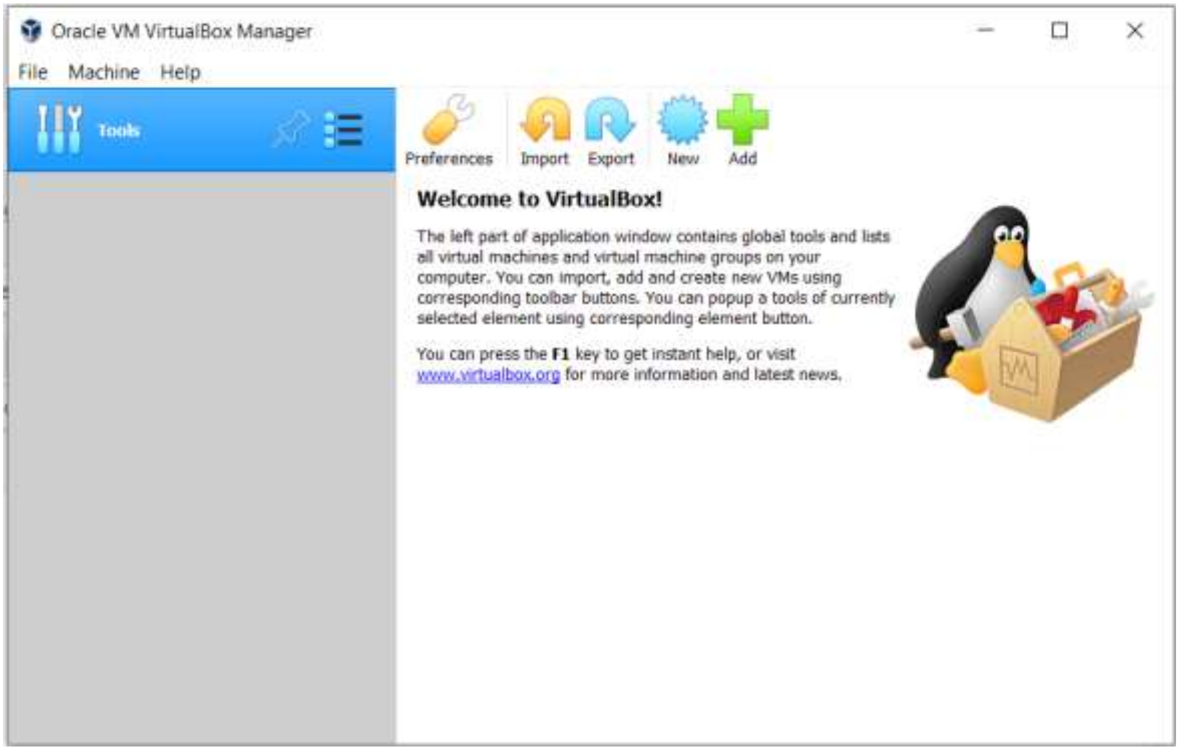


Oracle VM VirtualBox 6.1.2 installation is complete.

Click the Finish button to exit the Setup Wizard.

☑ Start Oracle VM VirtualBox 6.1.2 after installation

7. After clicking on ‘Finish’, VirtualBox will open:



Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

Result:

VirtualBox has been installed on a Windows system.

PRACTICAL 2

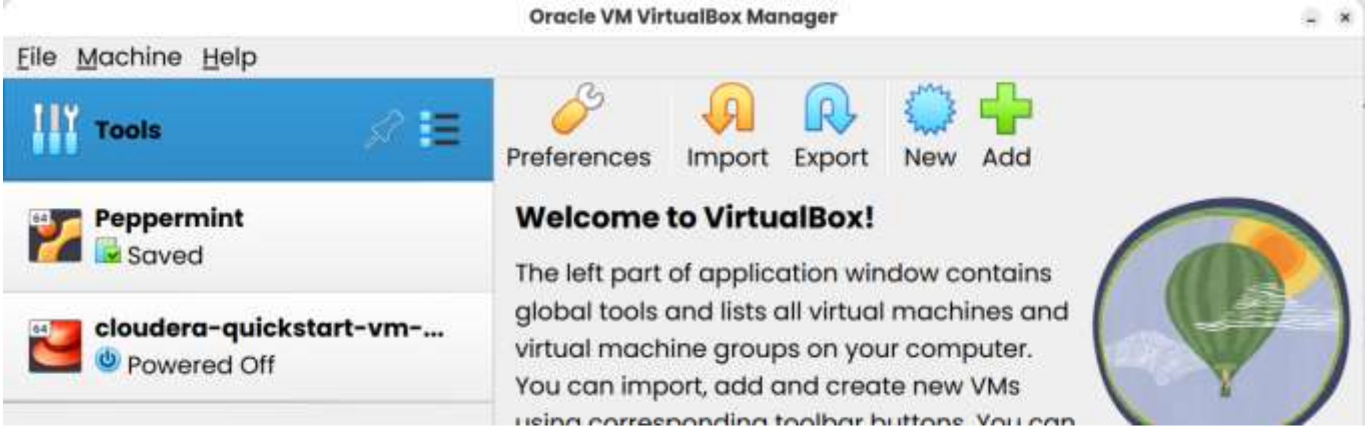
Aim: Create a Virtual Machine using VirtualBox

Introduction:

A virtual machine (VM) is a software-based simulation of a physical computer that runs an operating system and applications just like a real machine. It operates in an isolated environment using the host system's hardware resources. VMs allow multiple OSes to run simultaneously on a single physical device.

Procedure:

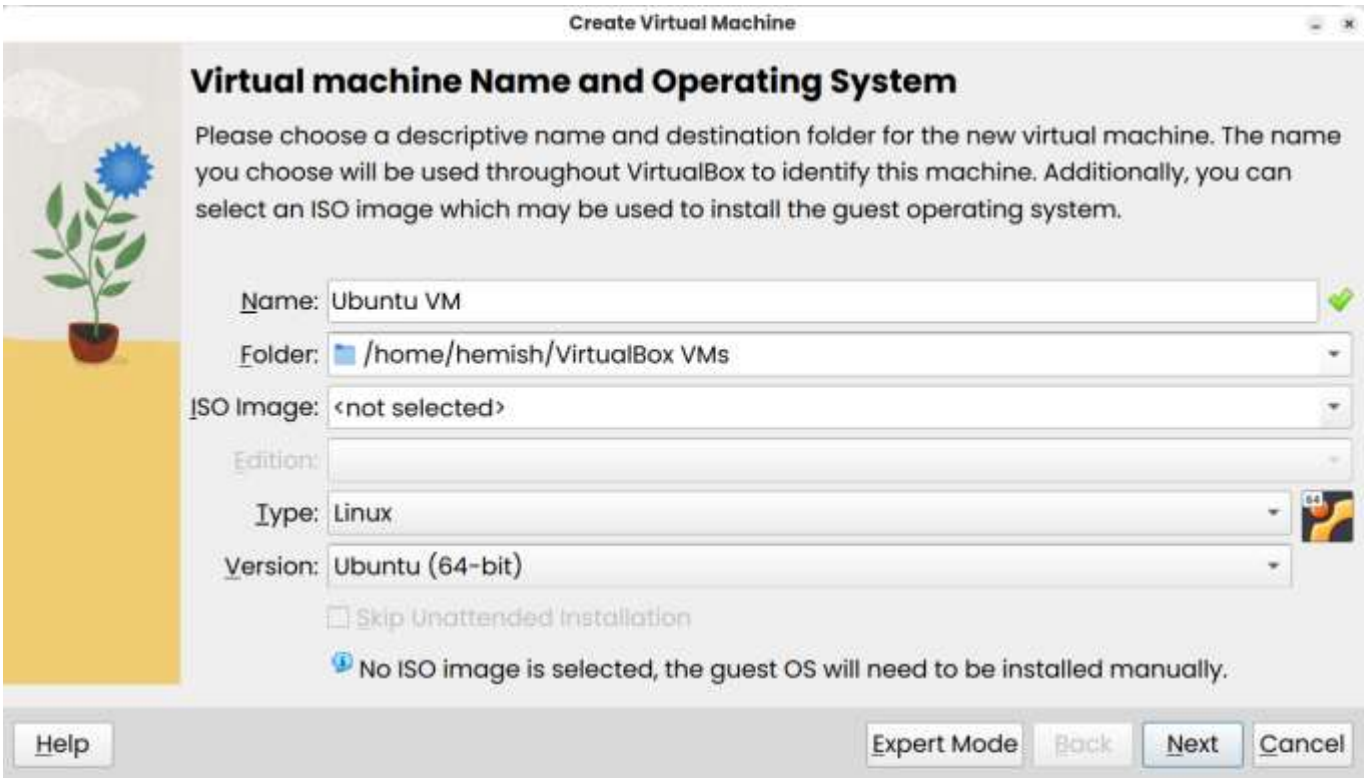
1. Open VirtualBox.



Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can

2. Click on 'New' button.



Virtual machine Name and Operating System

Please choose a descriptive name and destination folder for the new virtual machine. The name you choose will be used throughout VirtualBox to identify this machine. Additionally, you can select an ISO image which may be used to install the guest operating system.

Name: Ubuntu VM

Folder: /home/hemish/VirtualBox VMs

ISO Image: <not selected>

Edition:

Type: Linux

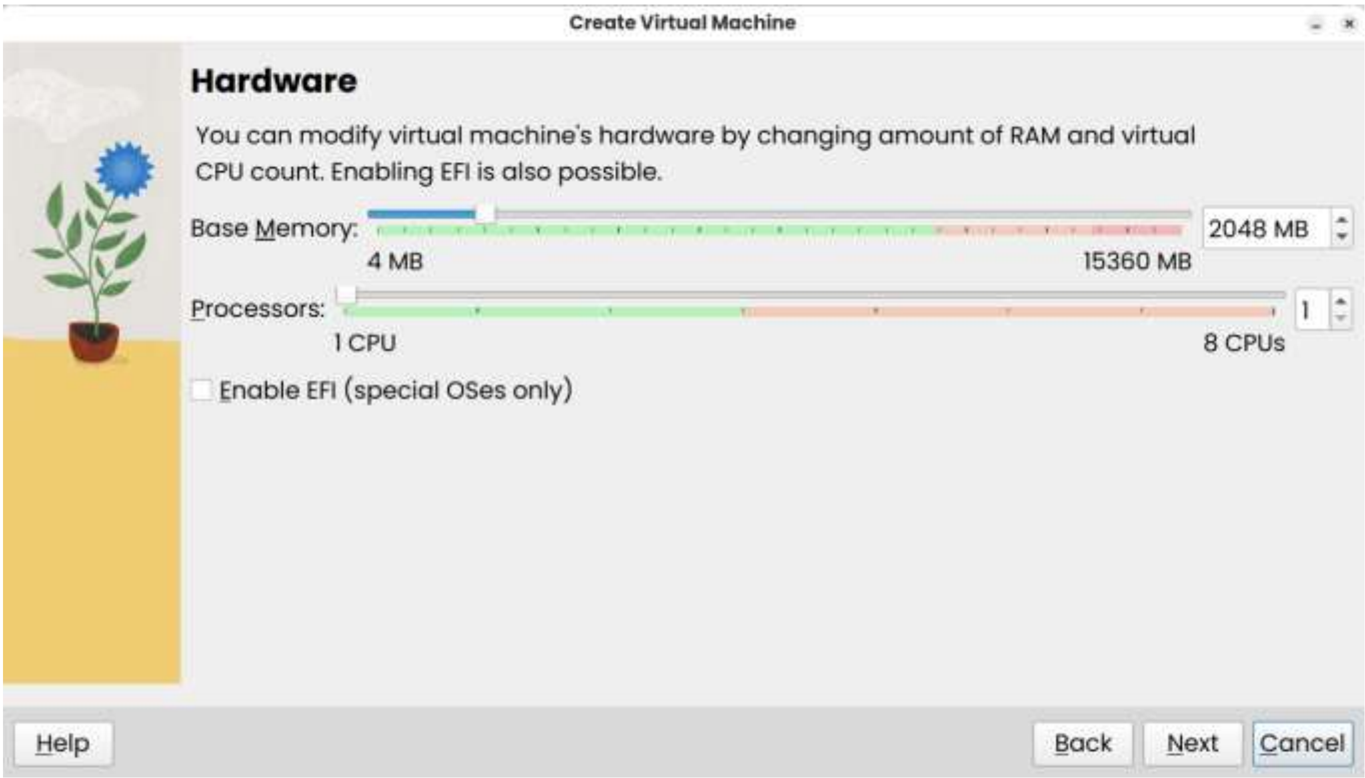
Version: Ubuntu (64-bit)

□ Skip Unattended Installation

No ISO image is selected, the guest OS will need to be installed manually.

3. Enter the name, say 'Ubuntu VM'. Select a location you want to store the VM to. In type, select 'Linux' and version as 'Ubuntu (64-bit)'.

4. Select the desired amount of base memory and number of processors to allocate, say 2048 MB memory and 1 processor.



Create Virtual Machine

Hardware

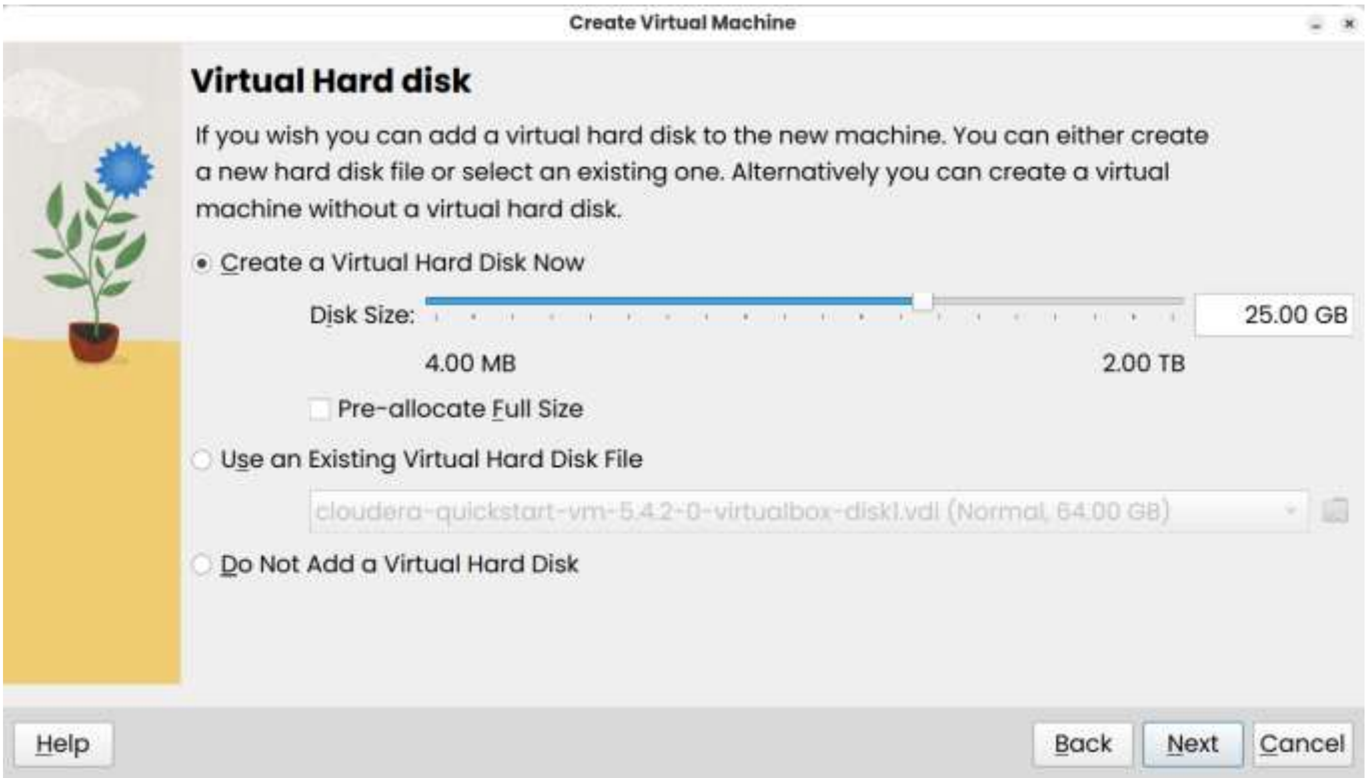
You can modify virtual machine's hardware by changing amount of RAM and virtual CPU count. Enabling EFI is also possible.

Base Memory: 2048 MB (4 MB – 15360 MB)

Processors: 1 (1 CPU – 8 CPUs)

□ Enable EFI (special OSes only)

5. Allocate the desired amount of space to create a virtual hard disk, say 25 GB.



Create Virtual Machine

Virtual Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select an existing one. Alternatively you can create a virtual machine without a virtual hard disk.

● Create a Virtual Hard Disk Now

Disk Size: 25.00 GB (4.00 MB – 2.00 TB)

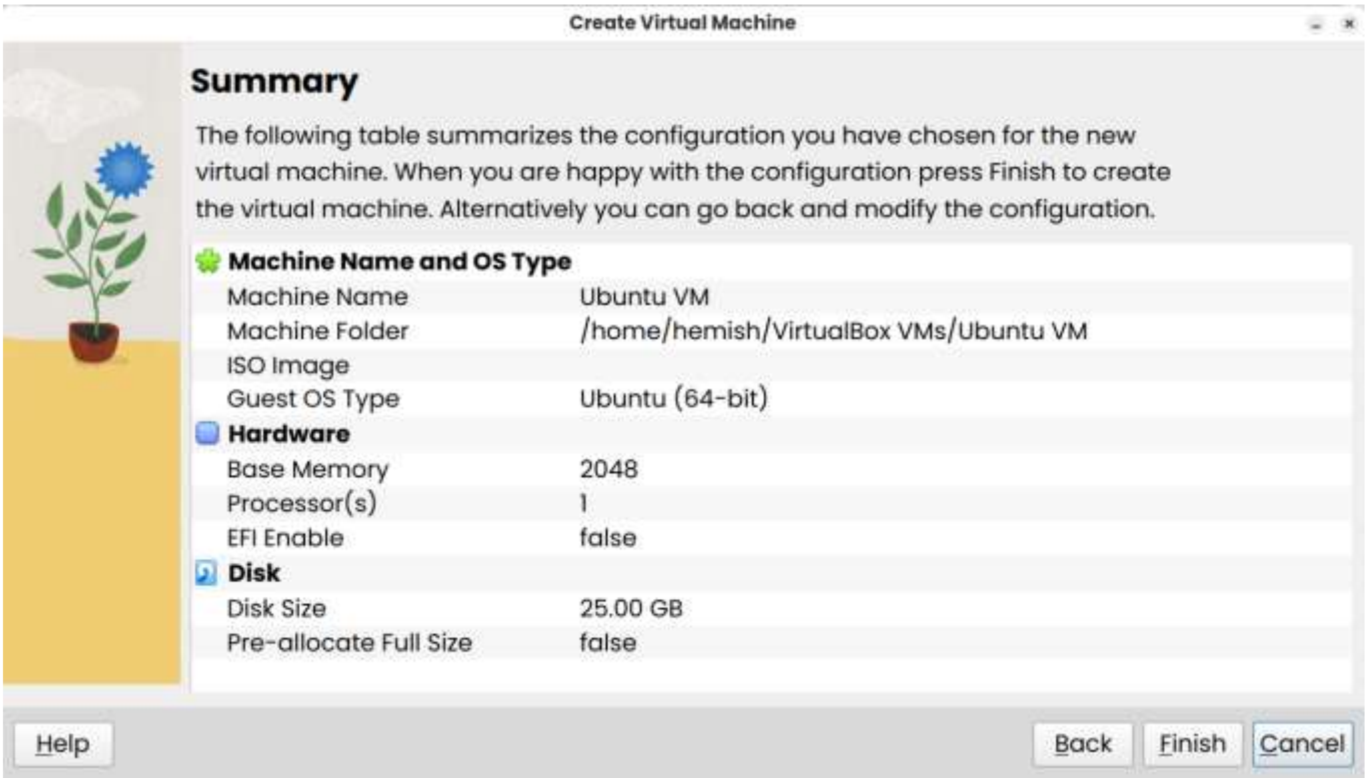
□ Pre-allocate Full Size

○ Use an Existing Virtual Hard Disk File

cloudera-quickstart-vm-5.4.2-0-virtualbox-disk1.vdi (Normal, 64.00 GB)

○ Do Not Add a Virtual Hard Disk

6. Review the details of the VM and click on 'Finish'.



Summary

The following table summarizes the configuration you have chosen for the new virtual machine. When you are happy with the configuration press Finish to create the virtual machine. Alternatively you can go back and modify the configuration.

Machine Name and OS Type	
Machine Name	Ubuntu VM
Machine Folder	/home/hemish/VirtualBox VMs/Ubuntu VM
ISO Image	
Guest OS Type	Ubuntu (64-bit)
Hardware	
Base Memory	2048
Processor(s)	1
EFI Enable	false
Disk	
Disk Size	25.00 GB
Pre-allocate Full Size	false

Result:

A new Virtual Machine has been created in VirtualBox.

PRACTICAL-3

Aim: Creation of AWS Free Tire account

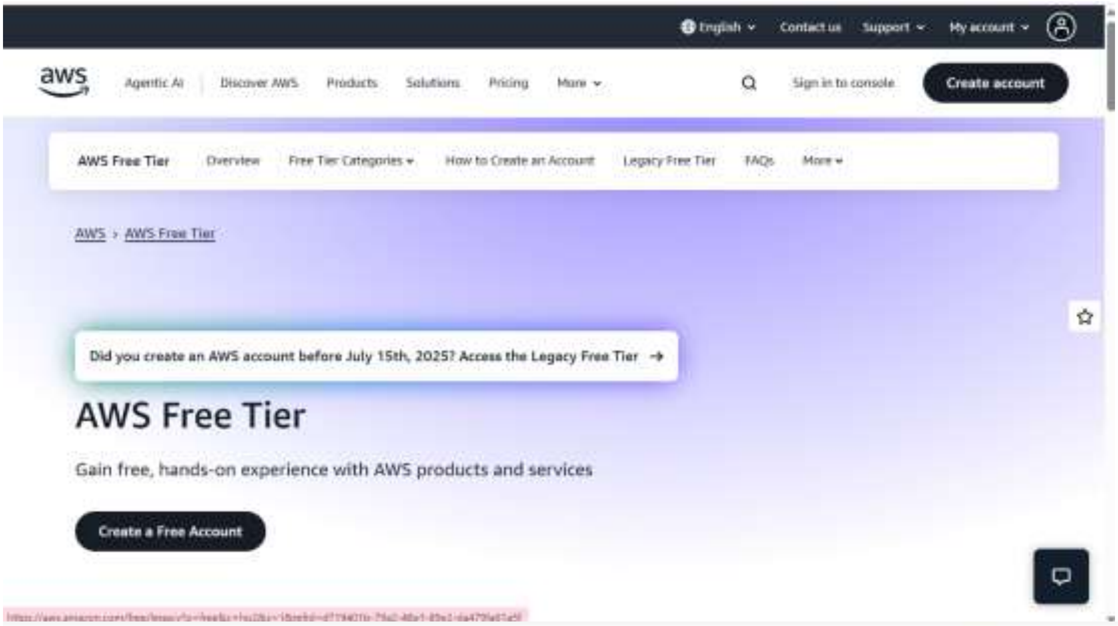
1. Open the link https://aws.amazom.com/
2. Click on Create an AWS Account.
3. Enter your email address and choose and account name then click on verify email address
4. Now, Enter the verification code you receive over your mail and click on verify.
5. Create a password for your account and proceed to the next step by clicking continue.
6. Now you have to fill in your personal information and under how do you plan to use AWS select personal and click on continue to proceed to the next step.
7. In this step you are required to fill in your card details in order to verify that you have an active bank account please do make sure that your card fulfills the below requirements

   a. Both credit and debit cards are allowed.

   b. Only cards from visa MasterCard, American express and Rupay global are accepted.

   c. Ensure international transactions are enabled for your card.

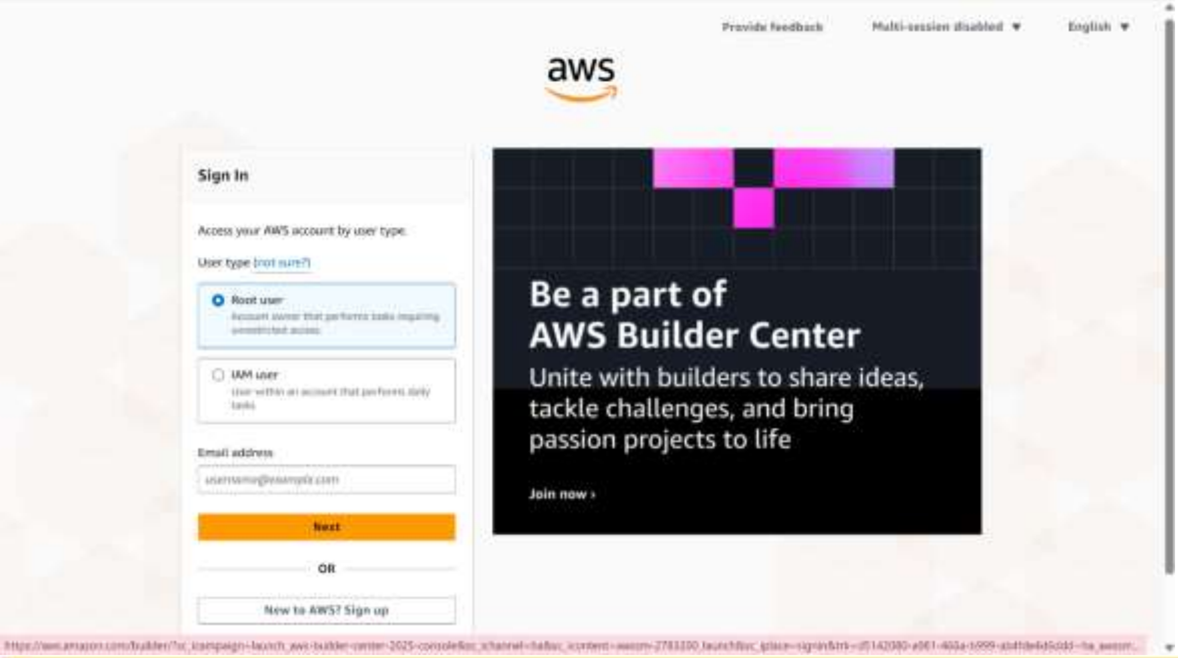
   d. E-Commerce transactions should also be enabled if there is no option for E-Commerce transactions make sure the channel type for your card is CNP
8. Now you need to verify your identity so you can select any of the options as in the screenshot and verify the same by entering the document details.
9. In this step you are required to verify your phone number that is contact details. Hence, fill in the same as well as captcha and click on verify.
10. Once done with verification choose a support plan we would recommend basic as it is free
11. Congratulations, you have successfully created your AWS account click on go to the AWS management console select a role and interest of your choice and proceed to login with the credentials you created by clicking sign in to the console at the top right



Did you create an AWS account before July 15th, 2025? Access the Legacy Free Tier →

AWS Free Tier

Gain free, hands-on experience with AWS products and services



Sign In

Access your AWS account by user type.

User type (not sure?)

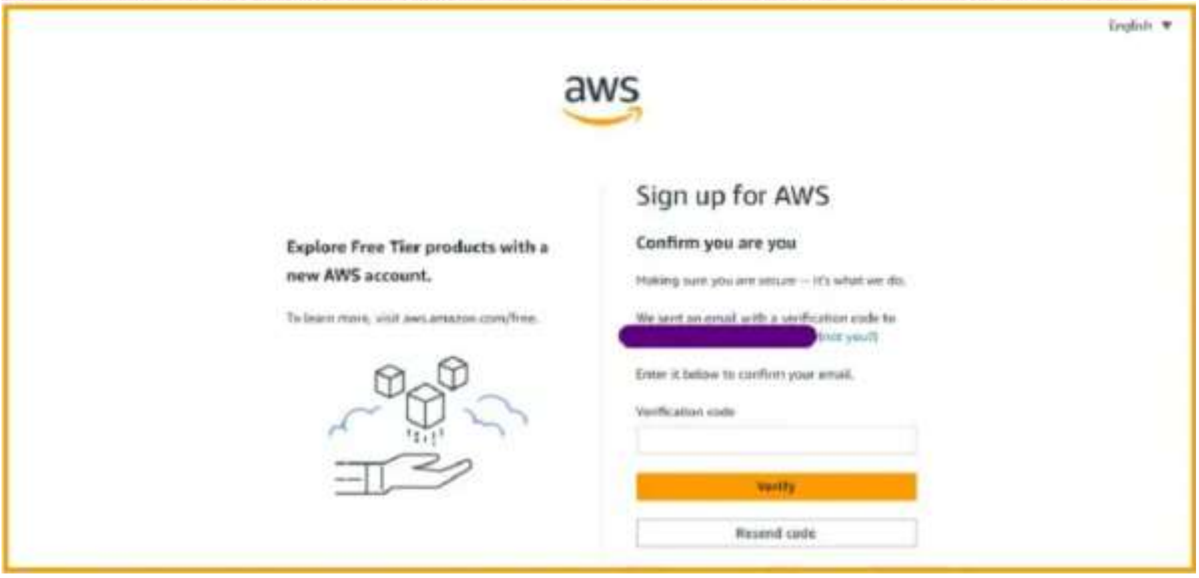
● Root user
Account owner that performs tasks requiring unrestricted access.

○ IAM user
User within an account that performs daily tasks.

Email address: username@example.com

Be a part of AWS Builder Center

Unite with builders to share ideas, tackle challenges, and bring passion projects to life



Explore Free Tier products with a new AWS account.

To learn more, visit aws.amazon.com/free.

Sign up for AWS

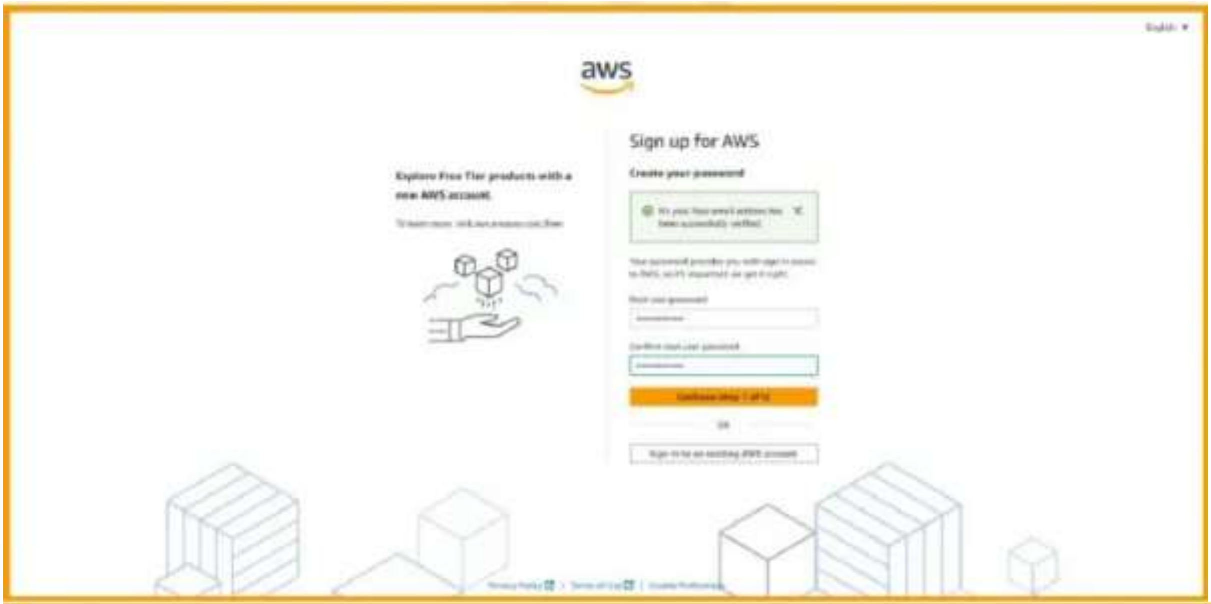
Confirm you are you

Making sure you are secure -- it's what we do.

We sent an email with a verification code to [redacted] (not you?)

Enter it below to confirm your email.

Verification code



English ▾

Sign up for AWS

Create your password

Hi, your free email address has been successfully verified. ✕

Your password provides you with sign in access to AWS, so it's important we get it right.

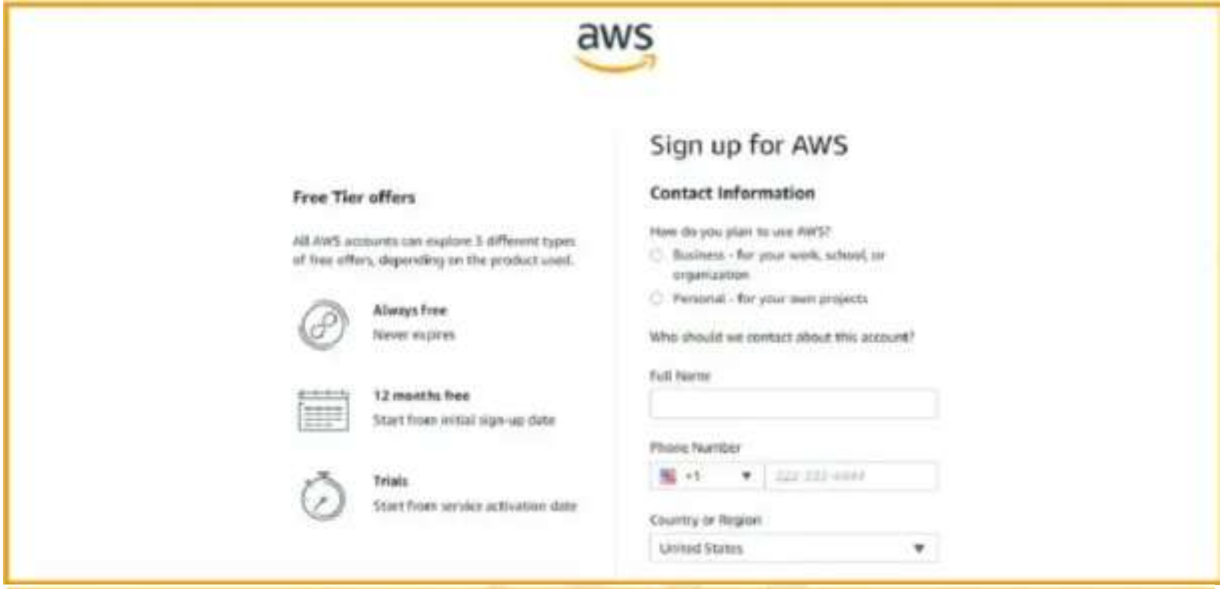
Root user password

Confirm root user password

Explore Free Tier products with a new AWS account.

To learn more, visit aws.amazon.com/free.

Continue (step 1 of 5)
or
Sign in to an existing AWS account
Privacy Policy | Terms of Use | Cookie Preferences



Sign up for AWS

Contact Information

How do you plan to use AWS?

○ Business - for your work, school, or organization

○ Personal - for your own projects

Who should we contact about this account?

Full Name

Phone Number

+1 ▾ 222-333-4444

Country or Region

United States ▾

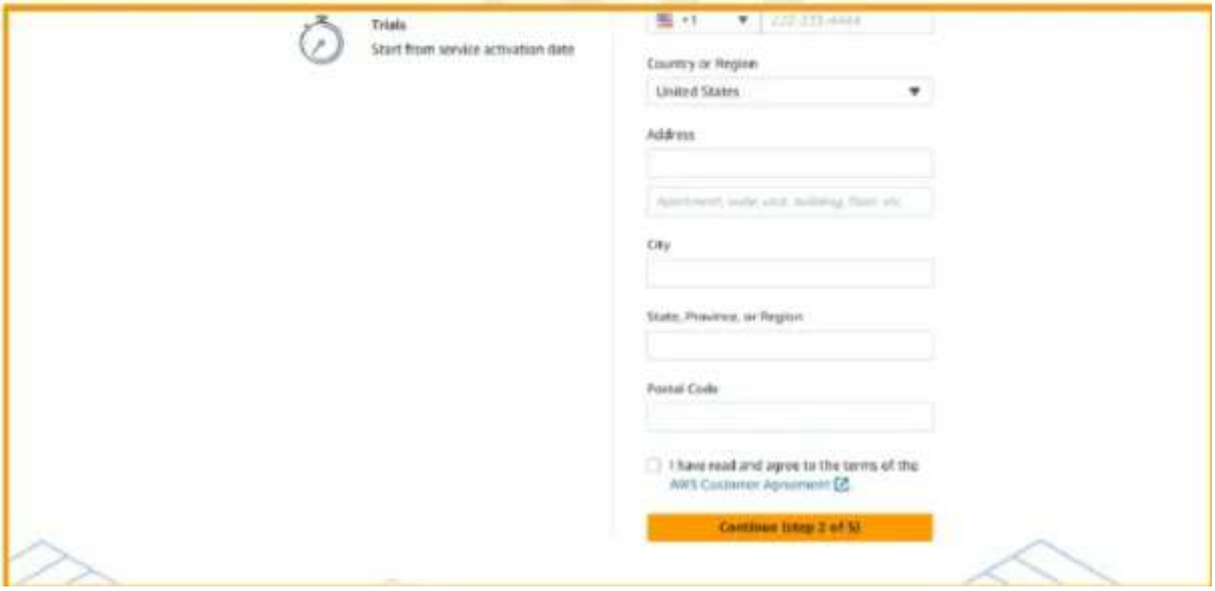
Free Tier offers

All AWS accounts can explore 3 different types of free offers, depending on the product used.

Always free
Never expires

12 months free
Start from initial sign-up date

Trials
Start from service activation date



Trials
Start from service activation date

+1 ▾ 222-333-4444

Country or Region

United States ▾

Address

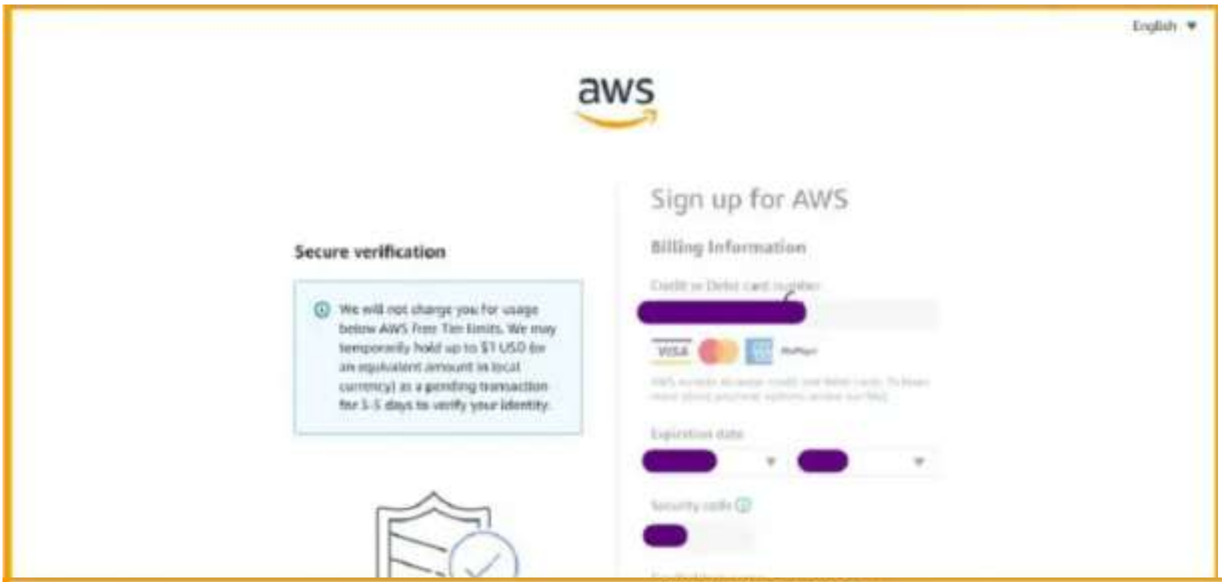
Apartment, suite, unit, building, floor, etc.

City

State, Province, or Region

Postal Code

□ I have read and agree to the terms of the AWS Customer Agreement



Secure verification

ⓘ We will not charge you for usage below AWS Free Tier limits. We may temporarily hold up to $1 USD (or an equivalent amount in local currency) as a pending transaction for 3-5 days to verify your identity.

Sign up for AWS

Billing Information

Credit or Debit card number

[redacted]

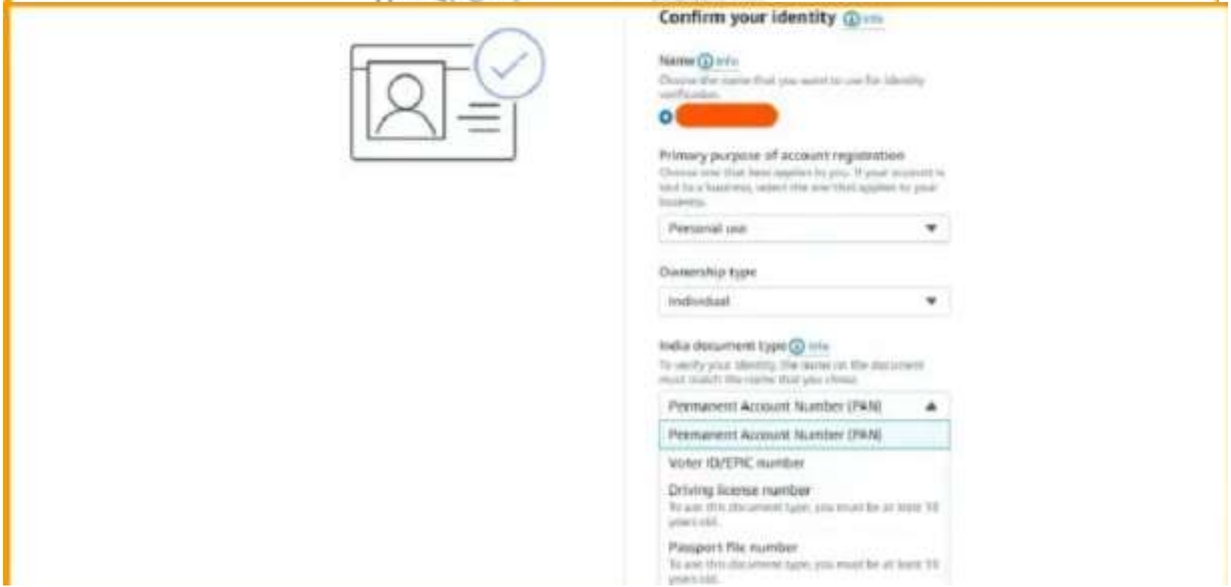
AWS accepts all major credit and debit cards. To learn more about payment options, review our FAQ.

Expiration date

[redacted] ▾ [redacted] ▾

Security code ⓘ

[redacted]



Confirm your identity ⓘ Info

Name ⓘ Info

Choose the name that you want to use for identity verification.

● [redacted]

Primary purpose of account registration

Choose one that best applies to you. If your account is tied to a business, select the one that applies to your business.

Personal use ▾

Ownership type

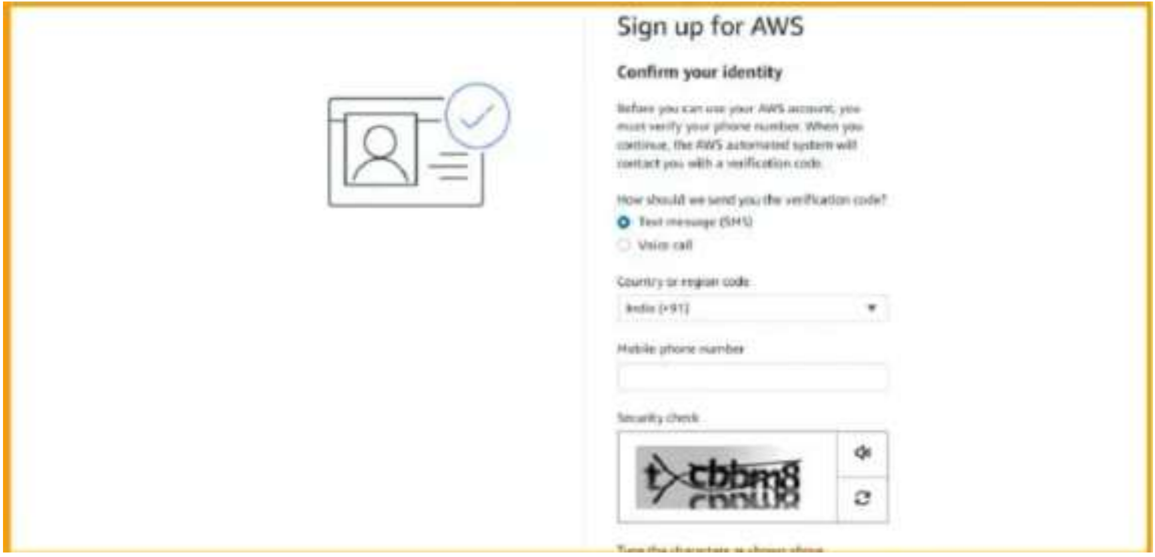
Individual ▾

India document type ⓘ Info

To verify your identity, the name on the document must match the name that you chose.

Permanent Account Number (PAN) ▴

- Permanent Account Number (PAN)
- Voter ID/EPIC number
- Driving license number
  To use this document type, you must be at least 18 years old.
- Passport File number
  To use this document type, you must be at least 18 years old.



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

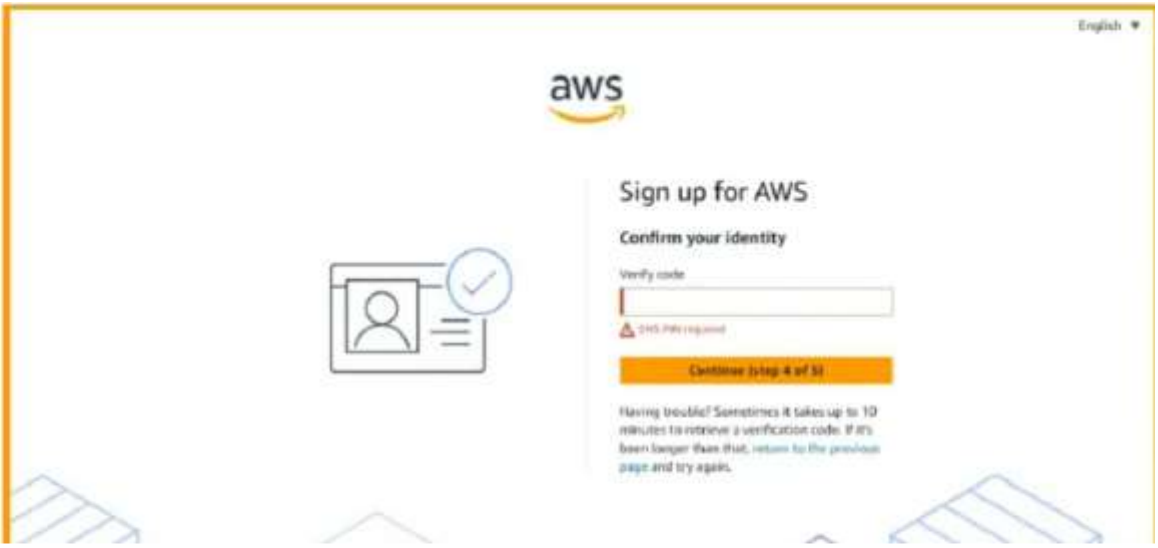
Country or region code

India (+91) ▾

Mobile phone number

Security check

Type the characters as shown above



English ▼

Sign up for AWS

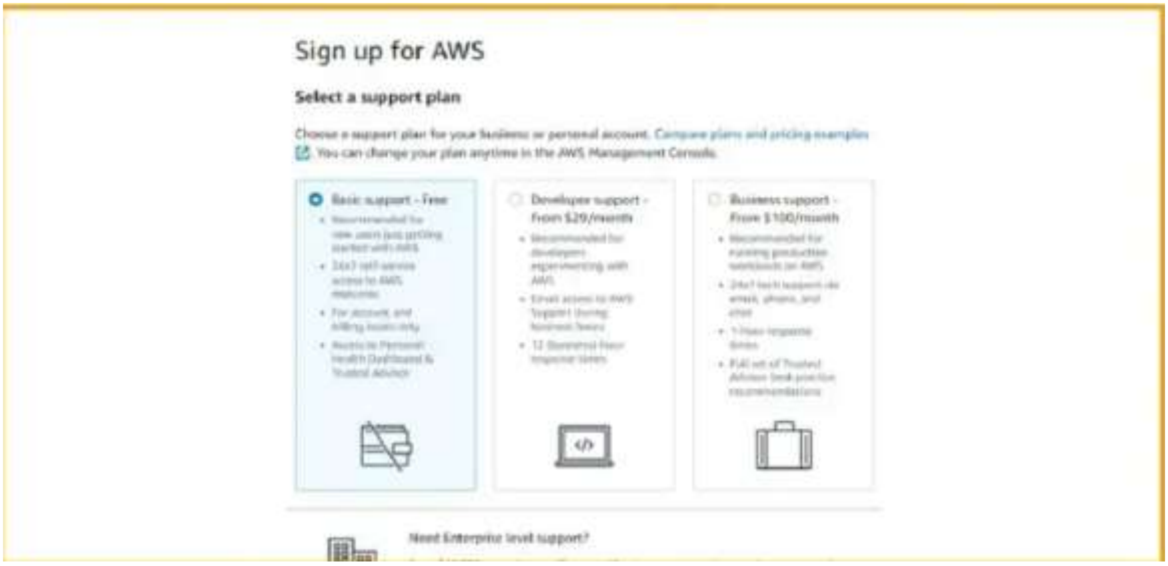
Confirm your identity

Verify code

⚠ SMS PIN required

Continue (step 4 of 5)

Having trouble? Sometimes it takes up to 10 minutes to retrieve a verification code. If it's been longer than that, return to the previous page and try again.



Sign up for AWS

Select a support plan

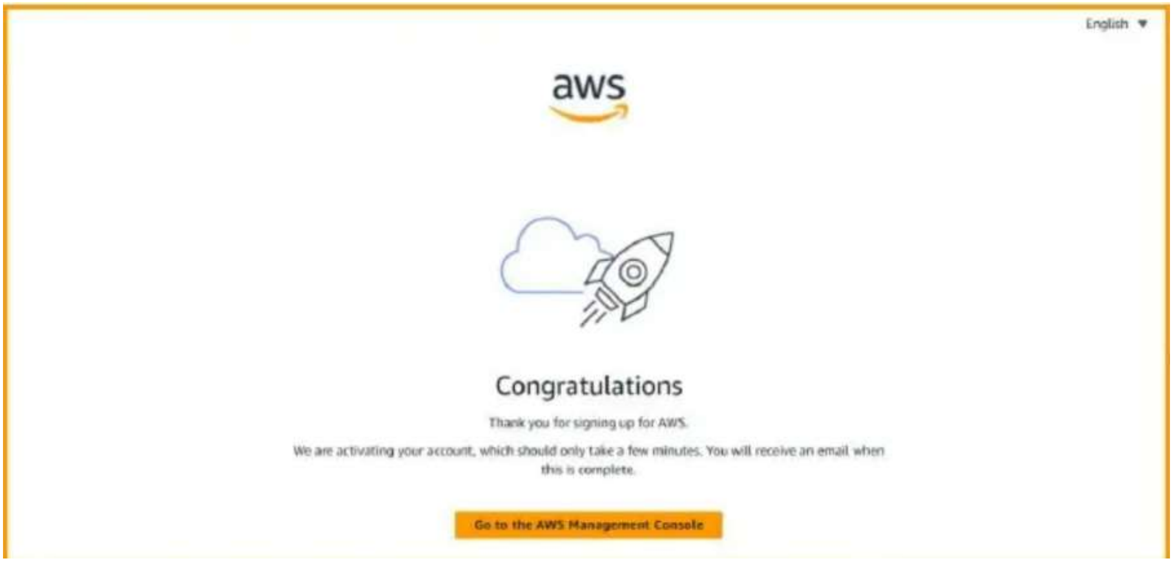
Choose a support plan for your business or personal account. Compare plans and pricing examples. You can change your plan anytime in the AWS Management Console.

● Basic support - Free
- Recommended for new users just getting started with AWS
- 24x7 self-service access to AWS resources
- For account and billing issues only
- Access to Personal Health Dashboard & Trusted Advisor

○ Developer support - From $29/month
- Recommended for developers experimenting with AWS
- Email access to AWS Support during business hours
- 12 (business) hour response times

○ Business support - From $100/month
- Recommended for running production workloads on AWS
- 24x7 tech support via email, phone, and chat
- 1-hour response times
- Full set of Trusted Advisor best-practice recommendations

Need Enterprise level support?



English ▼

Congratulations

Thank you for signing up for AWS.

We are activating your account, which should only take a few minutes. You will receive an email when this is complete.

Go to the AWS Management Console

PRACTICAL-4

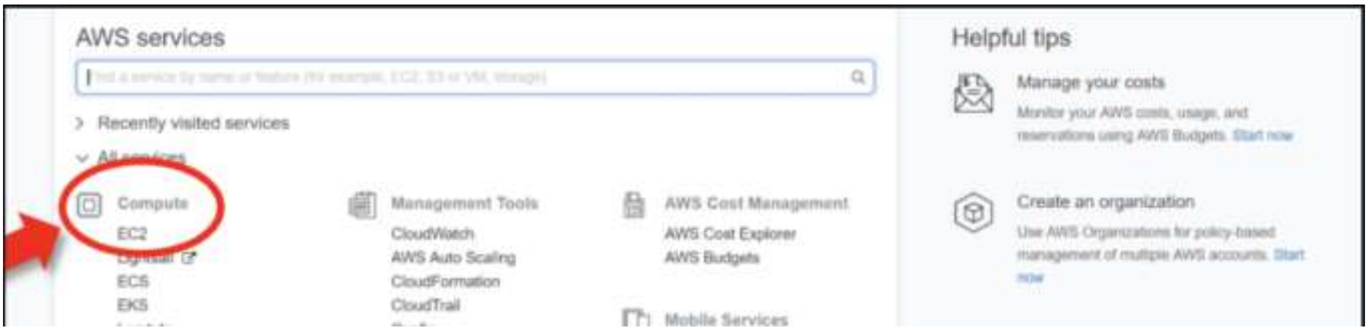
Aim: Creation of EC2 server

Steps to Create EC2 Instance in AWS (Amazon)

Follow the below steps to create an EC2 instance in AWS (Amazon):

Step 1: Login and Navigate to EC2 Dashboard

- Log in to your AWS Management Console.
- From the Services menu, choose EC2 under the Compute section.
- Under Resources, click Instances (Running) to view running instances (if any).



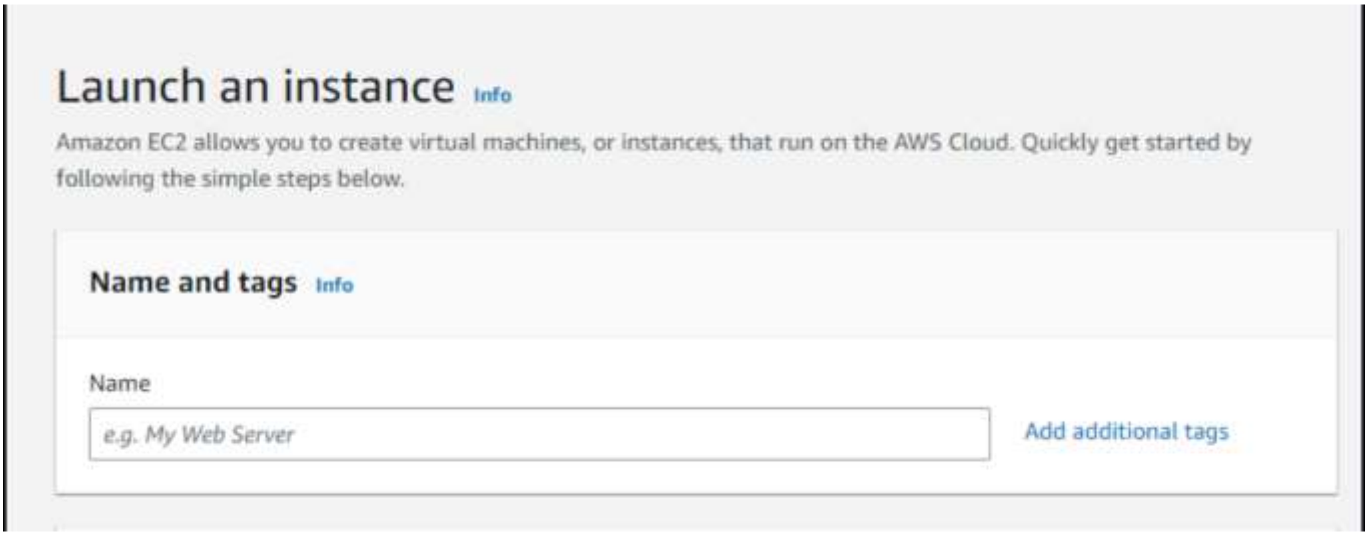
Monitor your AWS costs, usage, and reservations using AWS Budgets.

Use AWS Organizations for policy-based management of multiple AWS accounts.

Under Resources >> Click on "Instances running" -- It will show if any EC2 instances are running or not.

Step 2: Launch a New Instance

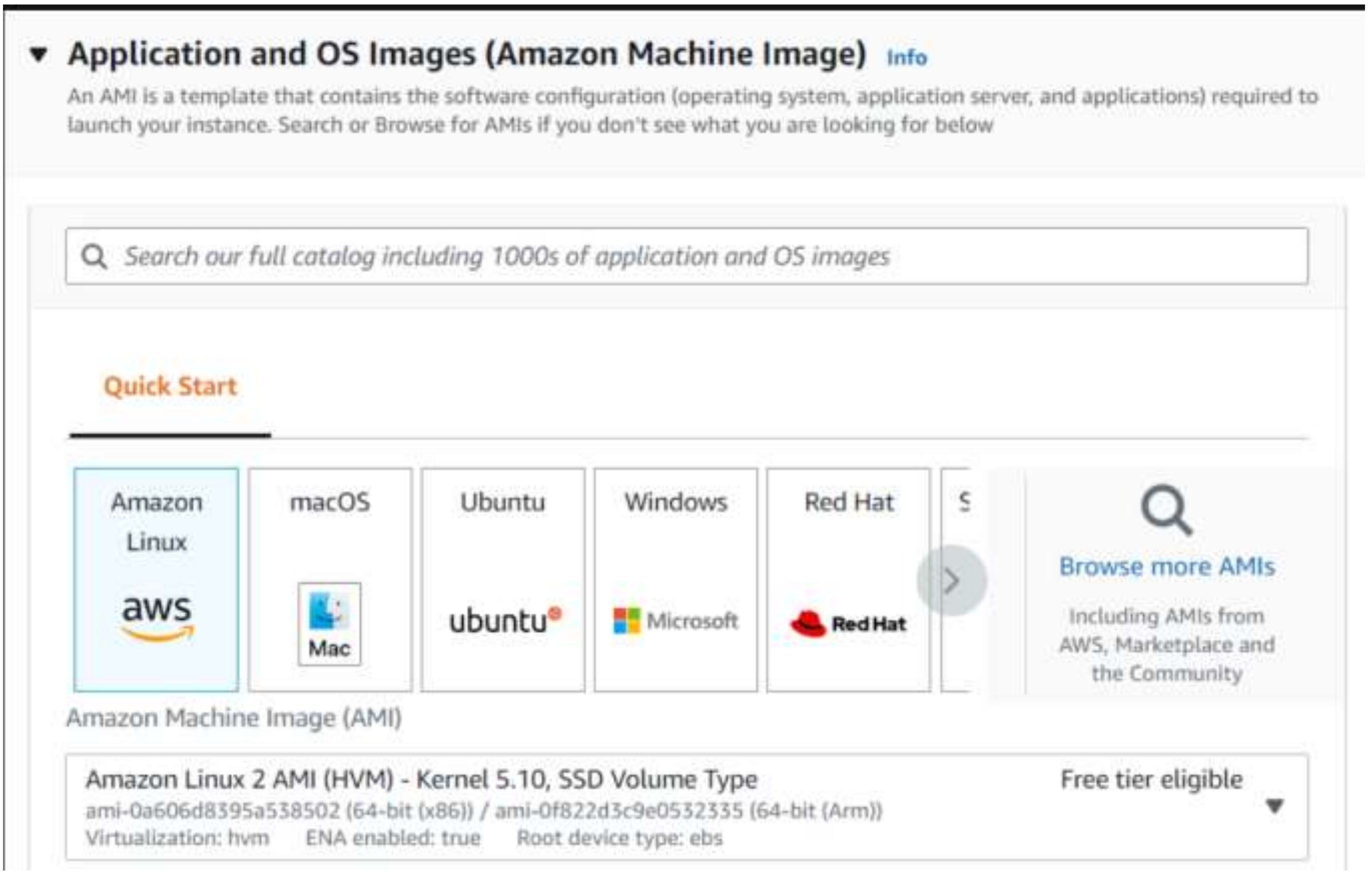
- Click **Launch Instance**.
- On the "Launch an Instance" page, enter a name for your instance (e.g., my-first-ec2-server).
- You'll now configure your server settings.



Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Step 3: Choose Amazon Machine Image

- Select an **Amazon Machine Image** (AMI), which is the OS for your server.
- For beginners, choose **Amazon Linux 2**, **Ubuntu**, or **Windows**, depending on your needs.
- AMIs come preconfigured with OS and some software like templates.



▾ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

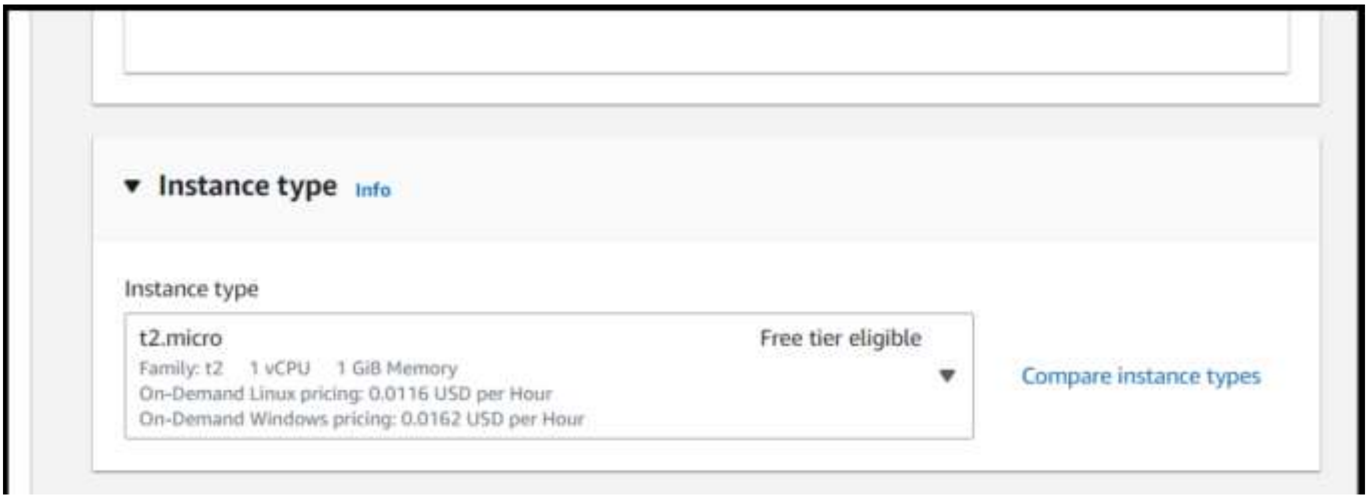
Search our full catalog including 1000s of application and OS images
Quick Start
Amazon Linux
aws
macOS
Mac
Ubuntu
ubuntu
Windows
Microsoft
Red Hat
Red Hat
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type — Free tier eligible
ami-0a606d8395a538502 (64-bit (x86)) / ami-0f822d3c9e0532335 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Step 4: Select Instance Type

- Select the **instance type** (defines CPU and memory).
- For Free Tier, choose **t2.micro** — 1 vCPU and 1 GB RAM.
- Avoid selecting higher types like t2.small, t3.medium, etc., unless needed, as they may incur charges.



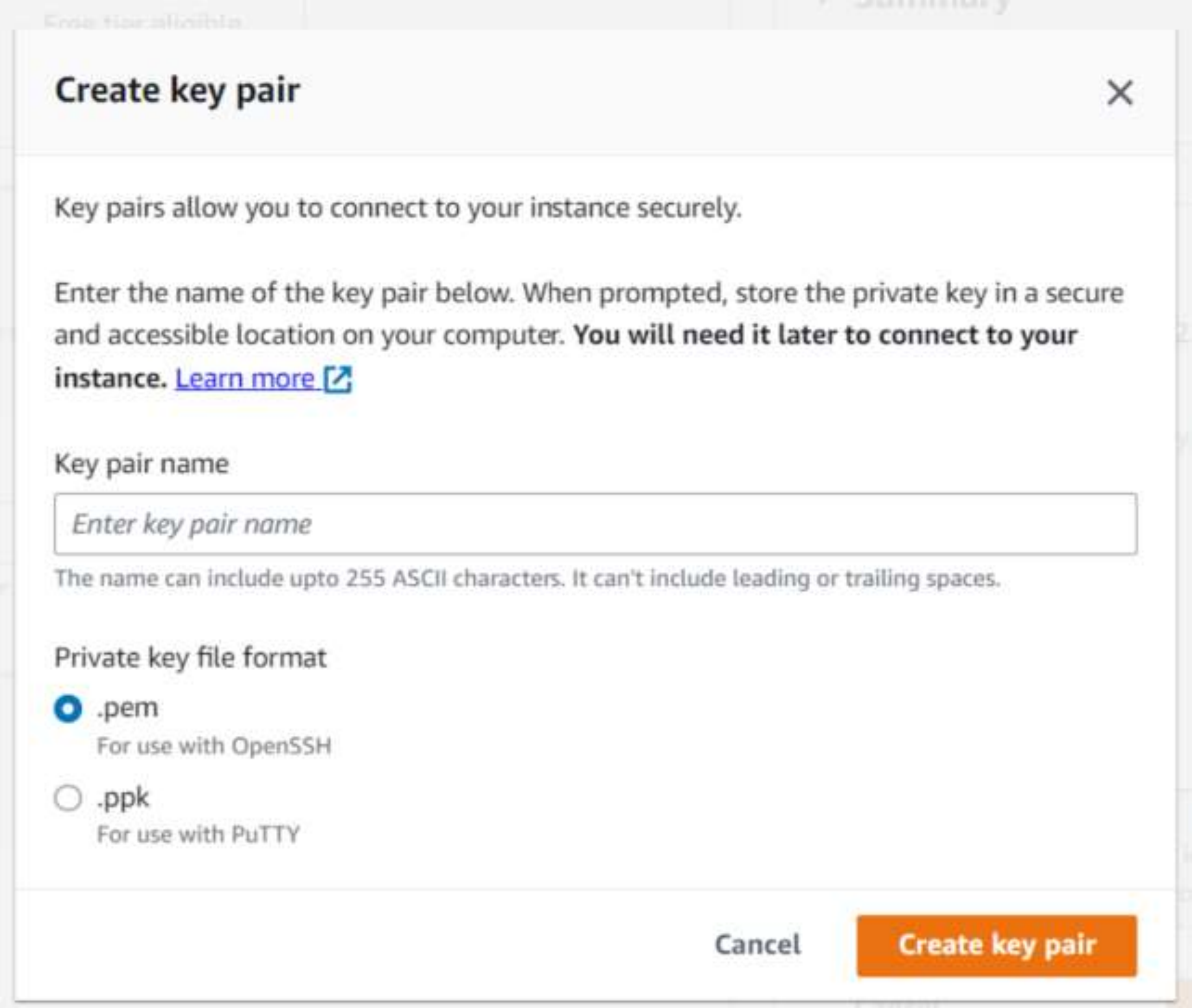
▾ Instance type Info

Instance type

t2.micro — Free tier eligible
Family: t2 1 vCPU 1 GiB Memory
On-Demand Linux pricing: 0.0116 USD per Hour
On-Demand Windows pricing: 0.0162 USD per Hour

Step 5: Configure Key Pair

1. EC2 instances use **SSH key pairs** for secure access.
2. Click **Create new key pair**:
   - Enter a name.
   - Choose file format: .pem for Linux/macOS or .ppk for Windows (for PuTTY).
   - Download the key file and **save it securely** (you won’t be able to download it again).
3. Select the created key pair from the dropdown.



Create key pair

Key pairs allow you to connect to your instance securely.

Enter the name of the key pair below. When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** Learn more

Key pair name

Enter key pair name

The name can include upto 255 ASCII characters. It can't include leading or trailing spaces.

Private key file format

● .pem
For use with OpenSSH

○ .ppk
For use with PuTTY

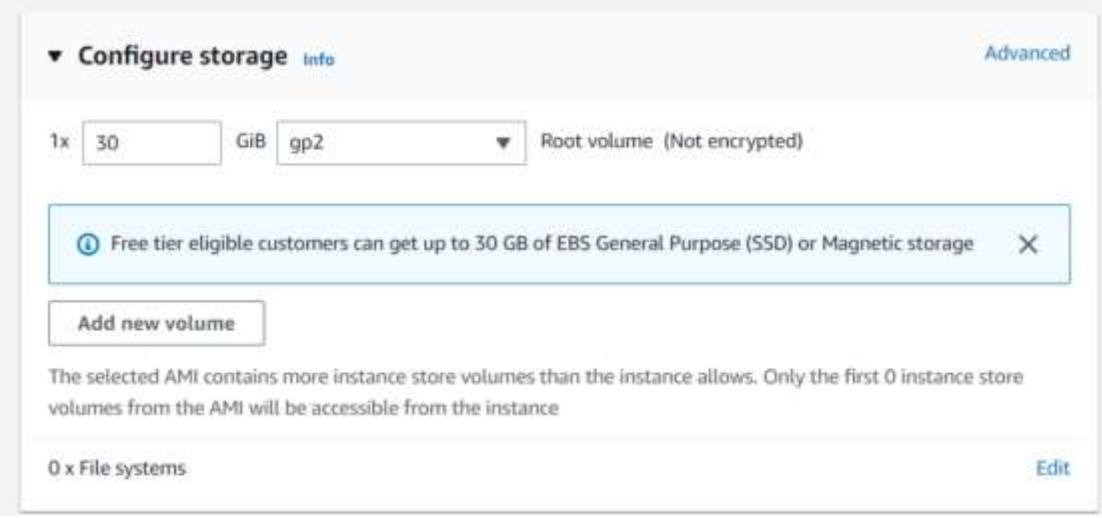
Step 6: Network and Storage Configuration

1. Network Settings: Use the default VPC and subnet unless you have specific networking needs.

2. Firewall (Security Group): Allow **SSH (port 22)** for Linux or **RDP (port 3389)** for Windows.

3. Storage Settings:

- Free Tier allows up to **30 GB of General Purpose SSD (gp2)**.
- Keep default (8 GB) or increase as needed.



▼ Configure storage Info

1x 30 GiB gp2 Root volume (Not encrypted)

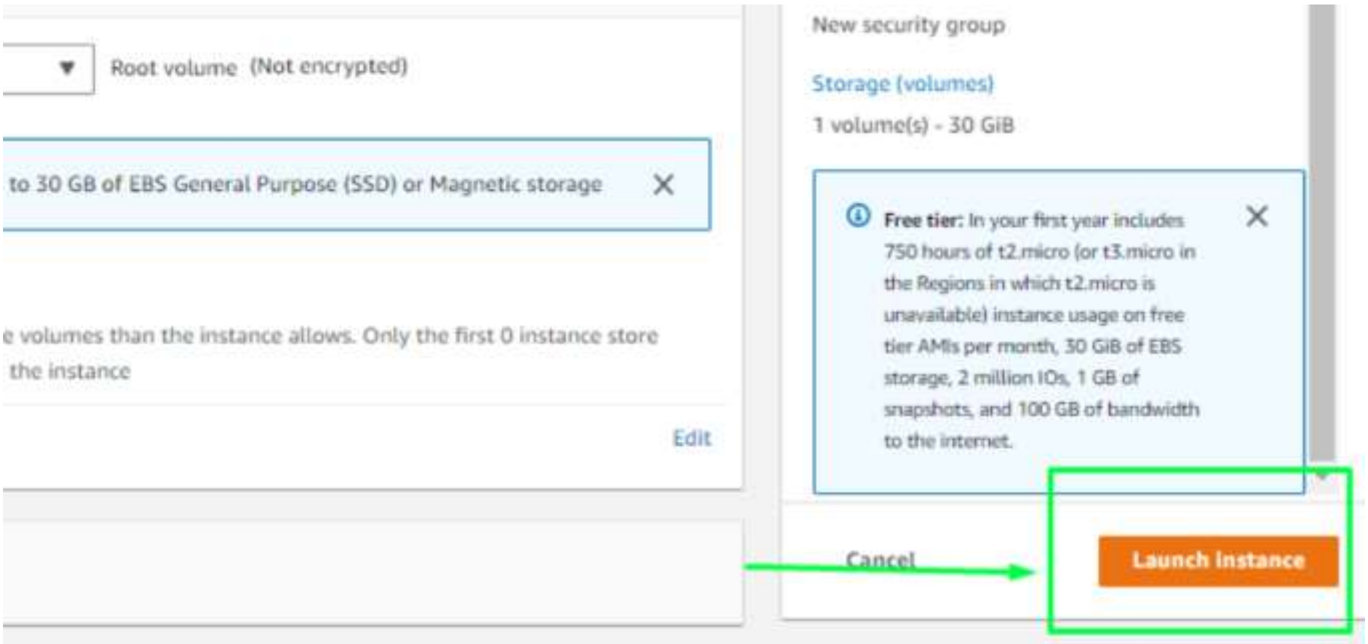
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance

0 x File systems

Step 7: Review and Launch

- Review all configurations to ensure they are **Free Tier eligible**.
- Click **Launch Instance**.
- You will see a confirmation page. Click **View Instances** to see your new server being initialized.
-


Root volume (Not encrypted)
to 30 GB of EBS General Purpose (SSD) or Magnetic storage ✕
e volumes than the instance allows. Only the first 0 instance store
the instance
Edit
New security group
Storage (volumes)
1 volume(s) - 30 GiB
Cancel
Launch instance

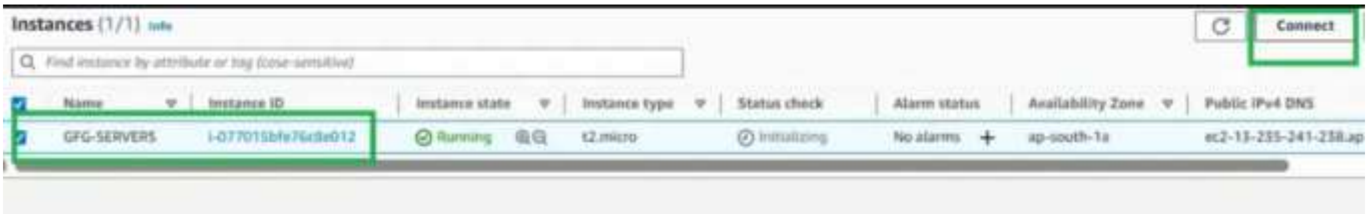
ⓘ **Free tier:** In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet. ✕

Steps to Connect Terminal Using SSH-Key

Once your instance is launched, secure access is essential. Follow the below steps to know how to connect using a terminal and your key pair.

Step 1: Locate Connection Details

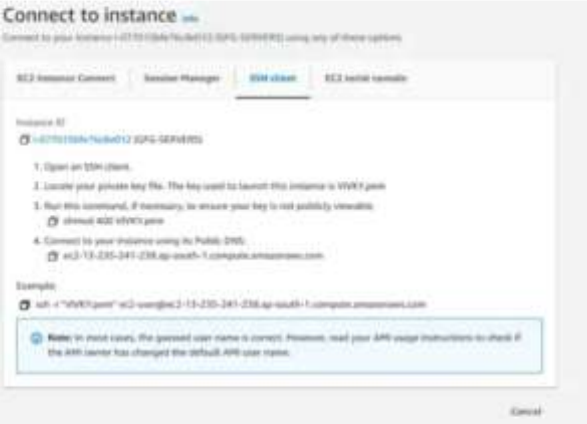
Select the server to which you want to connect and click on the connect button at the top of that instance as shown in the image below.



☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
☑	GFG-SERVERS	i-077015bfe76d8e012	Running	t2.micro	Initializing	No alarms +	ap-south-1a	ec2-13-235-241-238.ap

Step 2: Copy the SSH Command

Copy the SSH key which is right following the example it will acct as a key-pair to connect to EC2-Instance.



Connect to your instance i-077015bfe76d8e012 (GFG-SERVERS) using any of these options

Instance ID

i-077015bfe76d8e012 (GFG-SERVERS)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is VIVKY.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.

```
chmod 400 VIVKY.pem
```

4. Connect to your instance using its Public DNS:

```
ec2-13-235-241-238.ap-south-1.compute.amazonaws.com
```

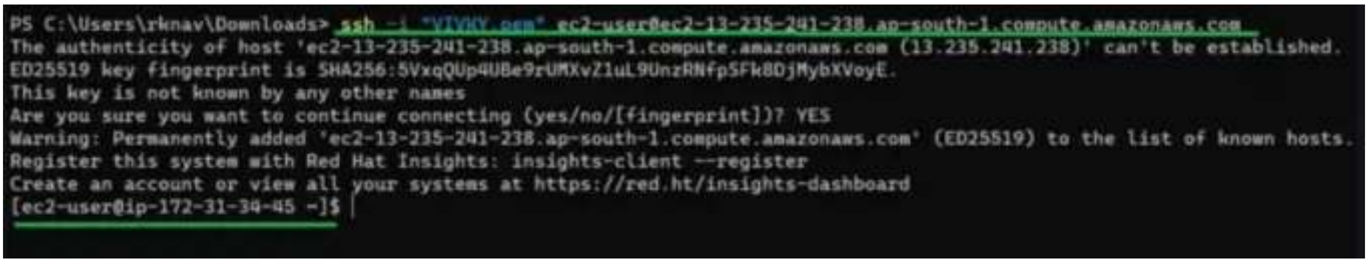
Example:

```
ssh -i "VIVKY.pem" ec2-user@ec2-13-235-241-238.ap-south-1.compute.amazonaws.com
```

Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

Step 3: Use Terminal

Open the terminal and go to the folder where your .pem file is located and paste the key that you have copied in AWS and paste it in the terminal.



```
PS C:\Users\rknav\Downloads> ssh -i "VIVKY.pem" ec2-user@ec2-13-235-241-238.ap-south-1.compute.amazonaws.com
The authenticity of host 'ec2-13-235-241-238.ap-south-1.compute.amazonaws.com (13.235.241.238)' can't be established.
ED25519 key fingerprint is SHA256:5VxqQUp4UBe9rUMXvZ1uL9UnzRNfpSFk8DjMybXVoyE.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? YES
Warning: Permanently added 'ec2-13-235-241-238.ap-south-1.compute.amazonaws.com' (ED25519) to the list of known hosts.
Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
[ec2-user@ip-172-31-34-45 ~]$ 
```

To know whether you connected to EC2-Instance perfectly or not you can check the IP-Address of the instance if the IP is displaying then you have connected successfully.

PRACTICAL-5

Aim: Creation of IAM User, Groups, Roles, Enabling MFA for Root User and IAM User

Step-by-Step Guide to Create an IAM User in AWS
Below is the step-by-step process you can follow to create an IAM user in AWS:

Step 1: Sign in to the AWS Console

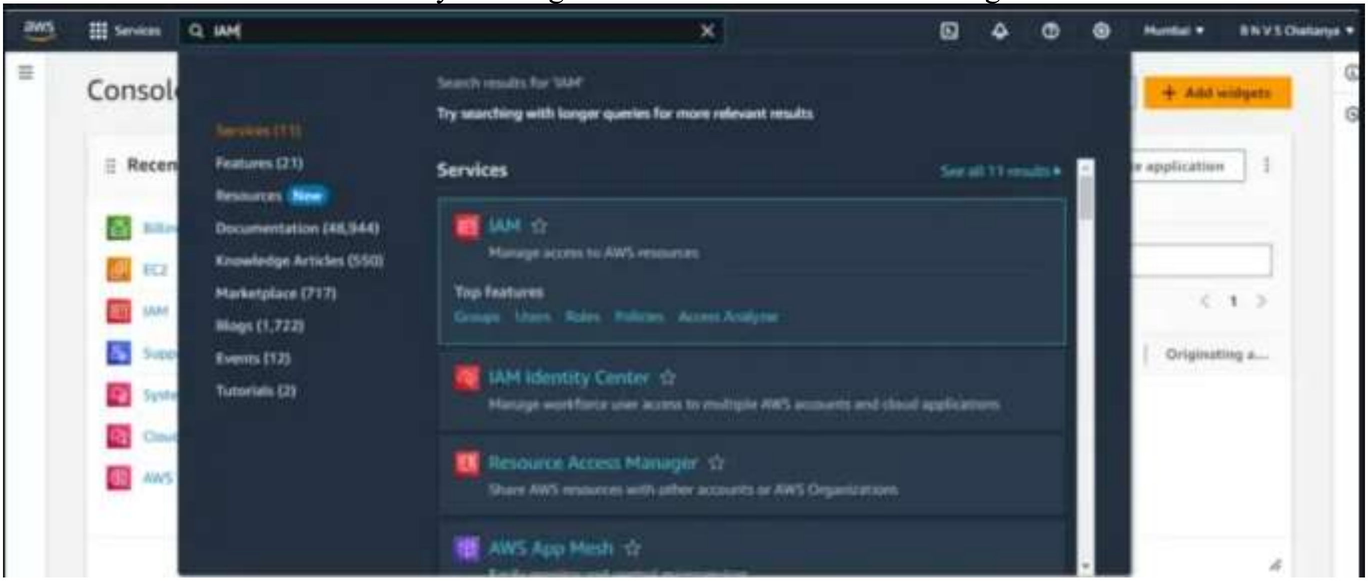
- Go to the Amazon Web Services Sign-In console.
- Create an AWS Free Tier Account.

Step 2: Log in as Root User

- Sign in using your root username and password**.**

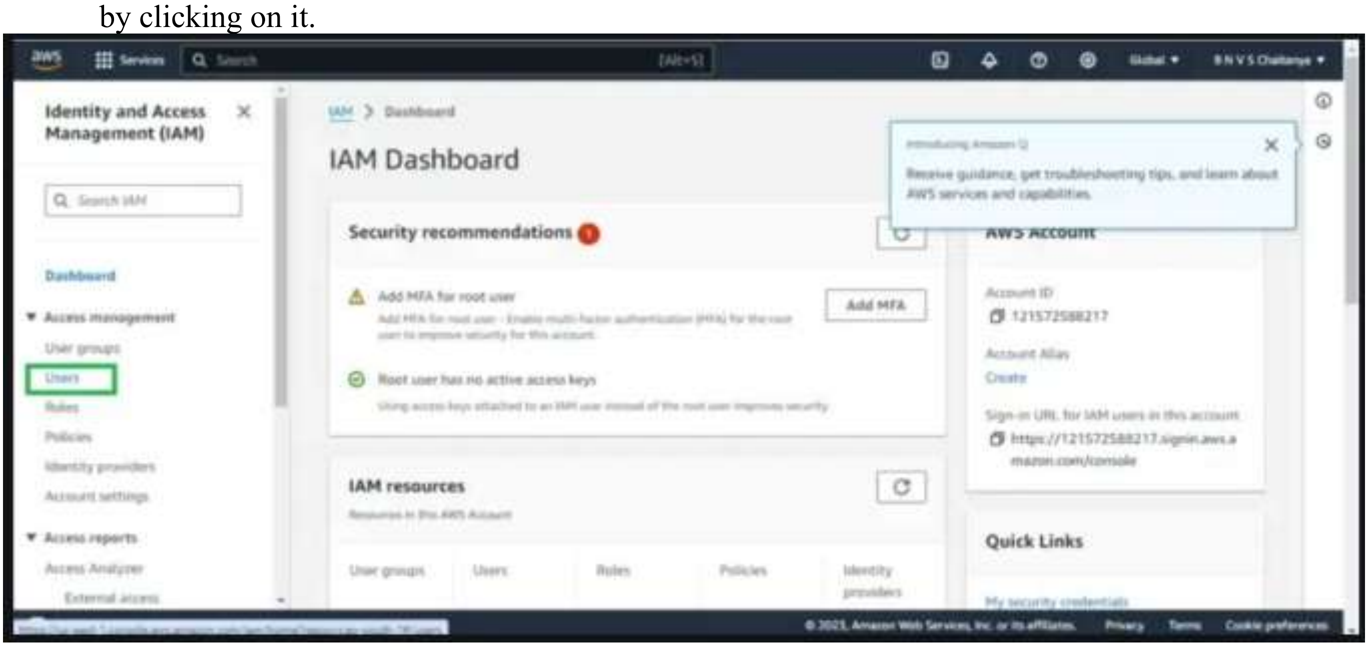
Step 3: Search for IAM

- Search in the search box by entering "IAM user" as shown in the image.



Step 4: Create a New IAM User

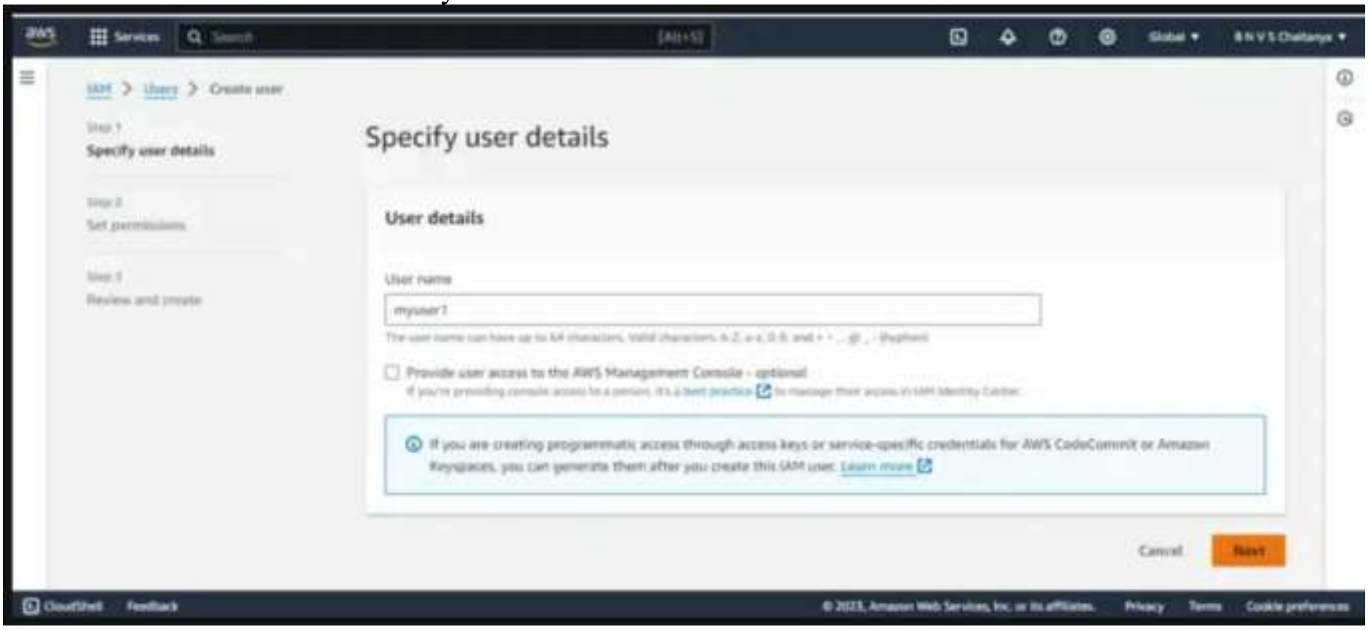
- After you enter the IAM user page, you can see the IAM dashboard then go to the "**users"** option by clicking on it.


Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
IAM > Dashboard
IAM Dashboard
Security recommendations
Add MFA for root user
Add MFA
Root user has no active access keys
IAM resources
Resources in this AWS Account
User groups Users Roles Policies Identity providers
AWS Account
Account ID
121572588217
Account Alias
Create
Sign-in URL for IAM users in this account
https://121572588217.signin.aws.amazon.com/console
Quick Links
My security credentials
© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

- In the user sections try creating a user by clicking on the "create user" button, now you will follow through with 3 phases for creating an IAM user.

i. Specifying the user details

- Provide the username that you would like to create as an IAM user



IAM > Users > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Specify user details

User details

User name: myuser1

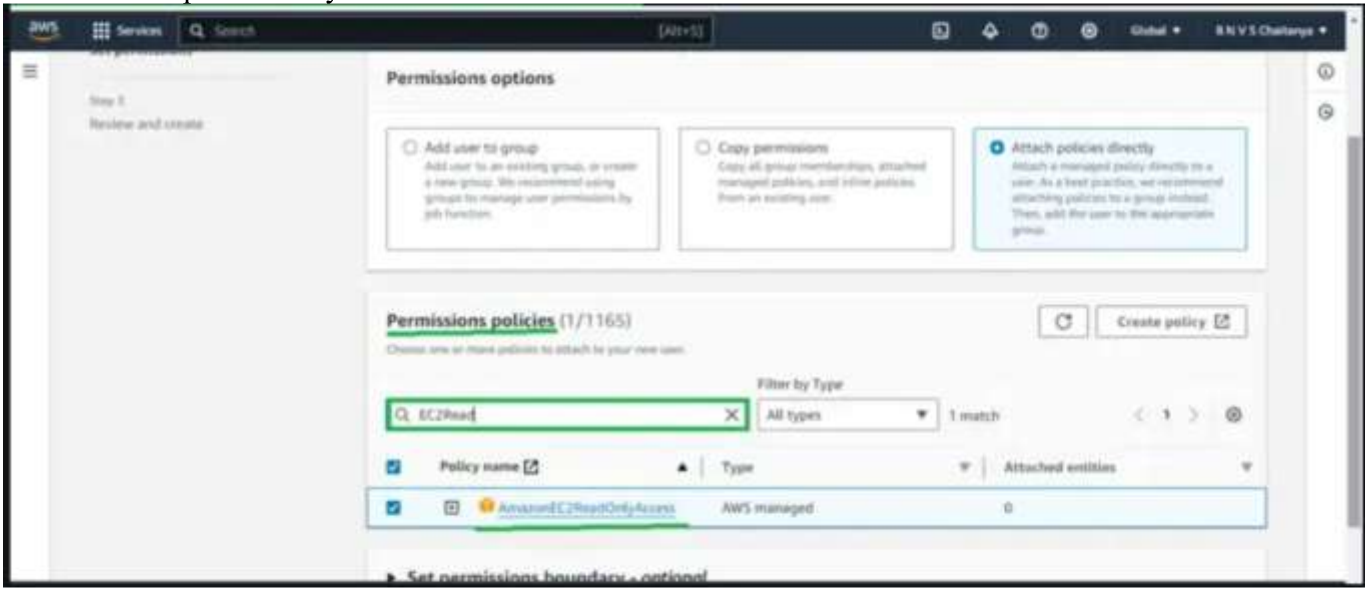
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☐ Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.

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

ii. Set Permissions

- Select the **attach policies directly** option, It is meant to assign the policies individually for the IAM user.
- In the **Permissions** policies section go to the search box and enter **EC2ReadOnly,** you will see the policy named **AmazonEC2ReadOnly** select it to provide this policy access to creating IAM user.
- Similarly you can add on whatever permissions that you would like from the pre-created policies as per the requirement.
- They will be a case in which we can't find the require based policies in that moment , you have to create policies as your own.



Step 3
Review and create

Permissions options

○ Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

○ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

● Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1/1165)

Choose one or more policies to attach to your new user.

Search: EC2Read

Filter by Type: All types

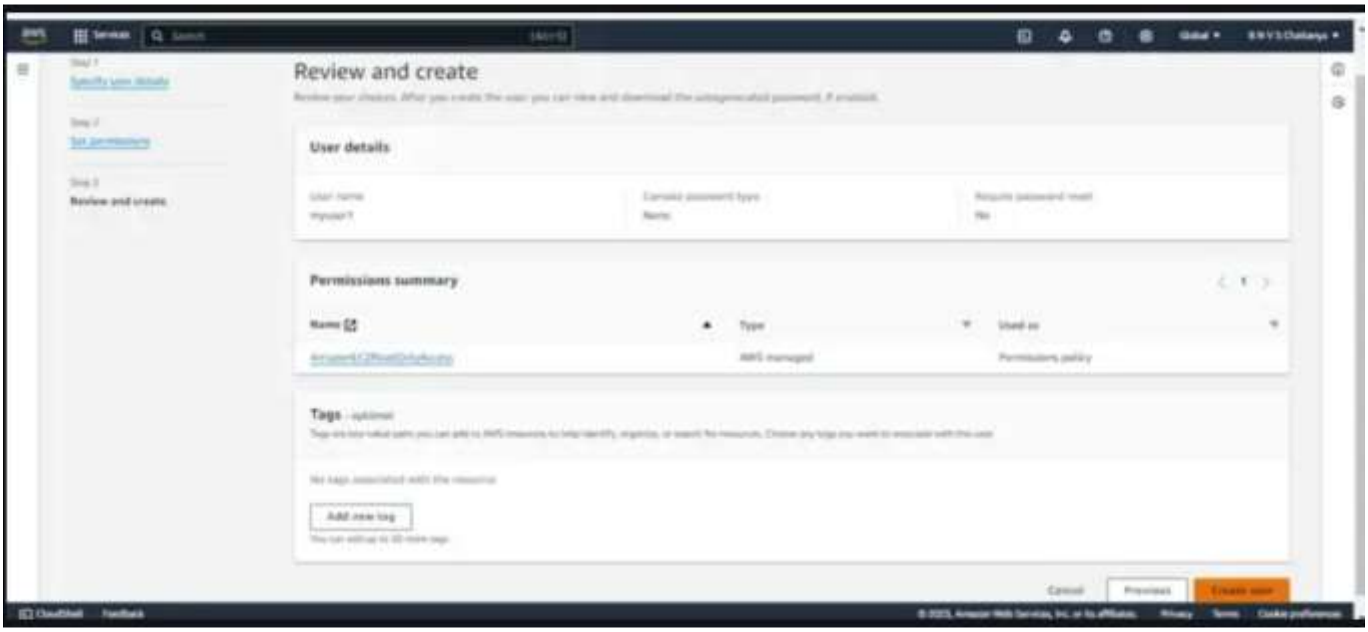
1 match

☑	Policy name	Type	Attached entities
☑	AmazonEC2ReadOnlyAccess	AWS managed	0

▸ Set permissions boundary - optional

iii. Review and Create

- In this step you have to review the information that you provided, once verified then go for the create option.



Review and create

User details

User name	Console password type	Require password reset
myuser1	None	No

Permissions summary

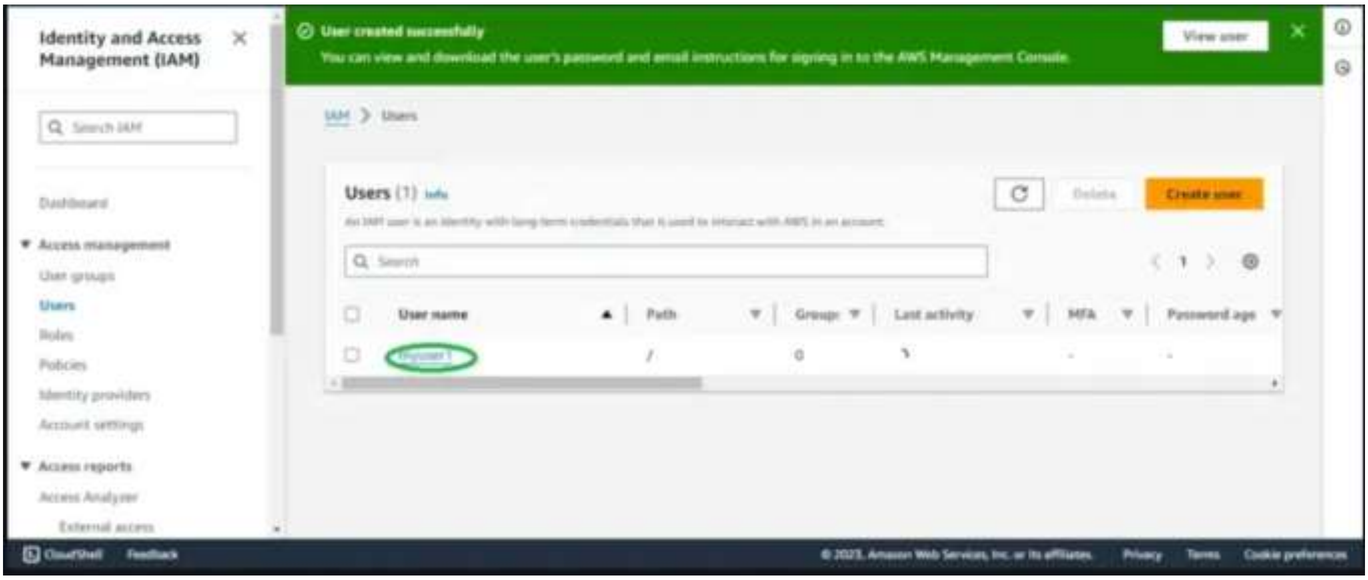
Name	Type	Used as
[illegible]	AWS managed	Permissions policy

Tags - optional

No tags associated with the resource.

- Finally, the IAM user is been created and you can see it on the dashboard as shown in the below figure.
-

Note: The user has now been created. The root user can later delete or modify its permissions if needed.



User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

Users (1)

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

□	User name	Path	Groups	Last activity	MFA	Password age
□	myuser1	/	0	[illegible]	-	-

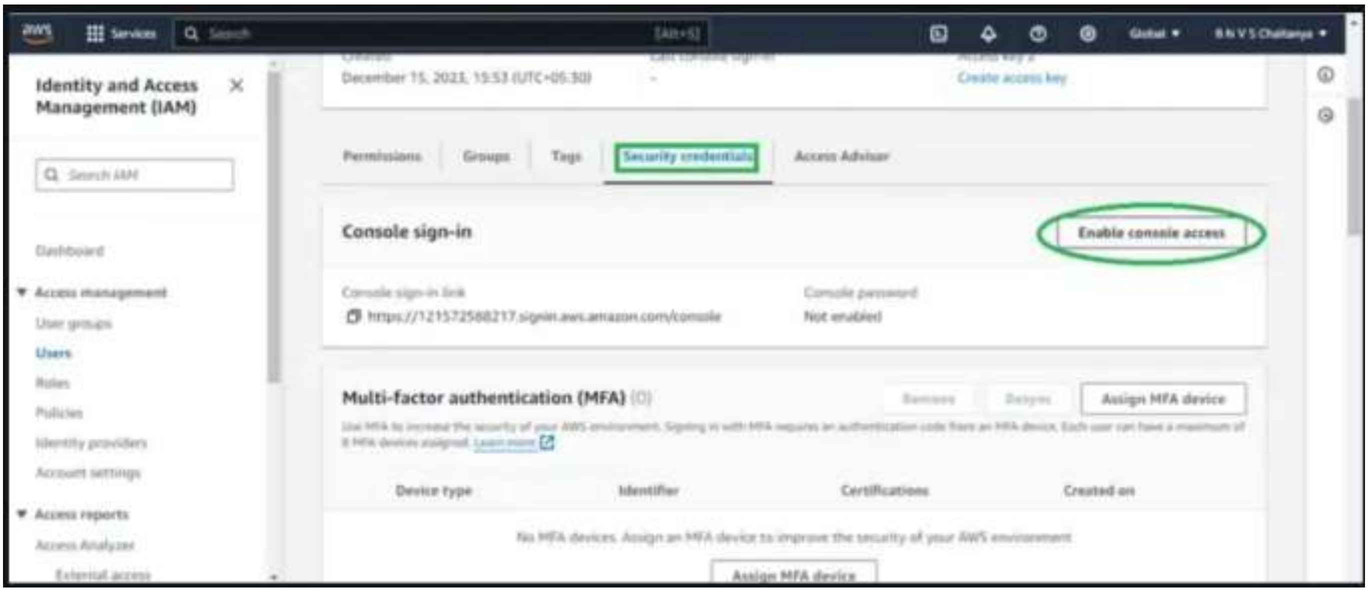
Step 5: Creating the Password (Security)

- Now based on the mode of login we have to create a password or access Key as per the use case. If you need a web console login then try on setting the password or else create the access key.

Note: In this article, I will guide you through web console access.

Step 6: Set Security Credentials

- Firstly Go to security credentials, In the console-sign-in section click on the enable console access button.



Identity and Access Management (IAM)

December 15, 2023, 15:53 (UTC+05:30)

Create access key

Permissions | Groups | Tags | Security credentials | Access Advisor

Console sign-in

Enable console access

Console sign-in link: https://121572588217.signin.aws.amazon.com/console

Console password: Not enabled

Multi-factor authentication (MFA) (0)

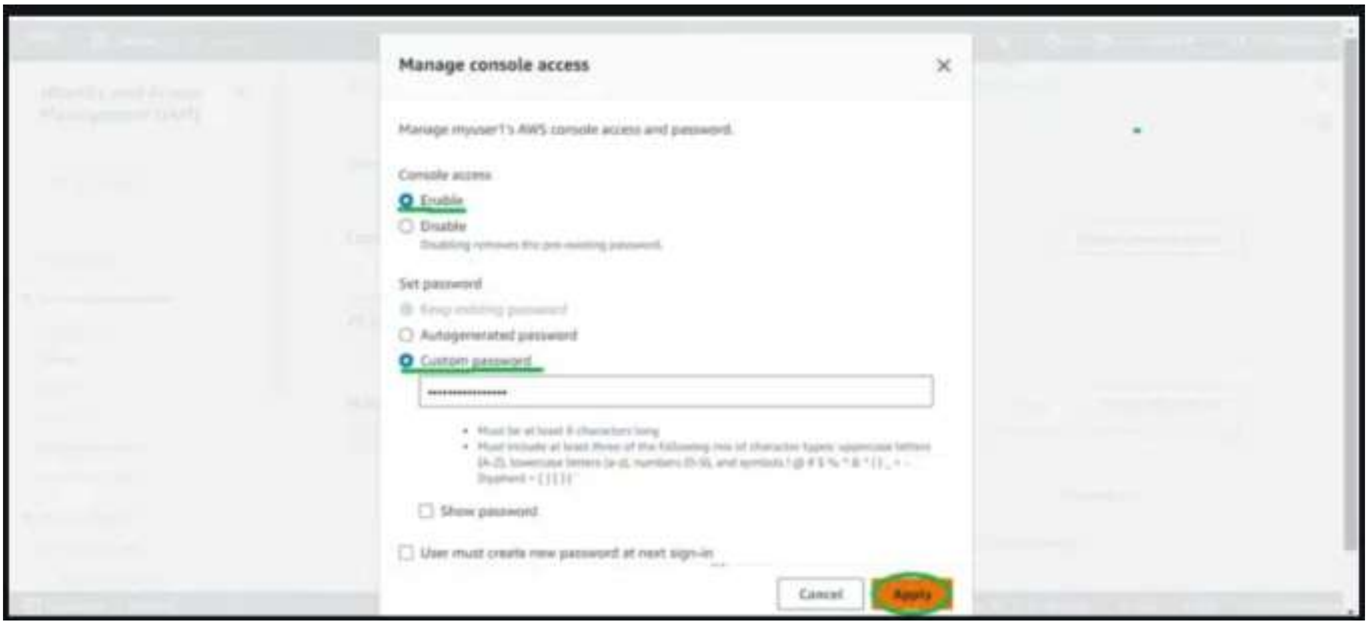
Assign MFA device

Device type	Identifier	Certifications	Created on

No MFA devices. Assign an MFA device to improve the security of your AWS environment.

By clicking on the Enable console button you will be redirected to manage console login as shown in figure:

- Choose the Enable option
- Coming to the below password section we can set either the customized password that is directly set now or auto-generating and try on creating at the time of login.
- Set a password that includes uppercase letters, lowercase letters, numbers, and special characters, as per AWS requirements.



Manage console access

Manage myuser1's AWS console access and password.

Console access

● Enable

○ Disable

Disabling removes the pre-existing password.

Set password

○ Keep existing password

○ Autogenerated password

● Custom password

- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '

□ Show password

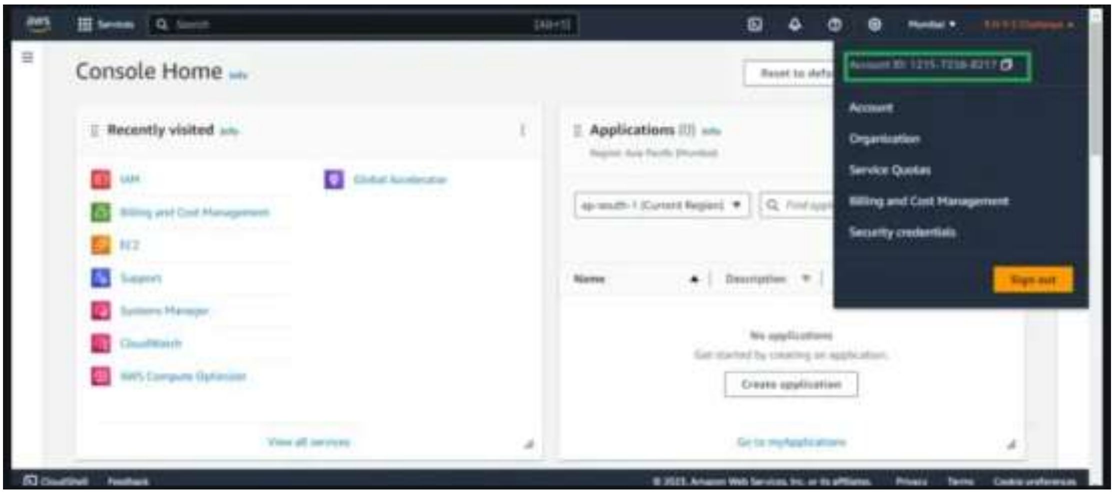
□ User must create new password at next sign-in

- Follow the instructions while setting the password once it is created click on 'Done' option.

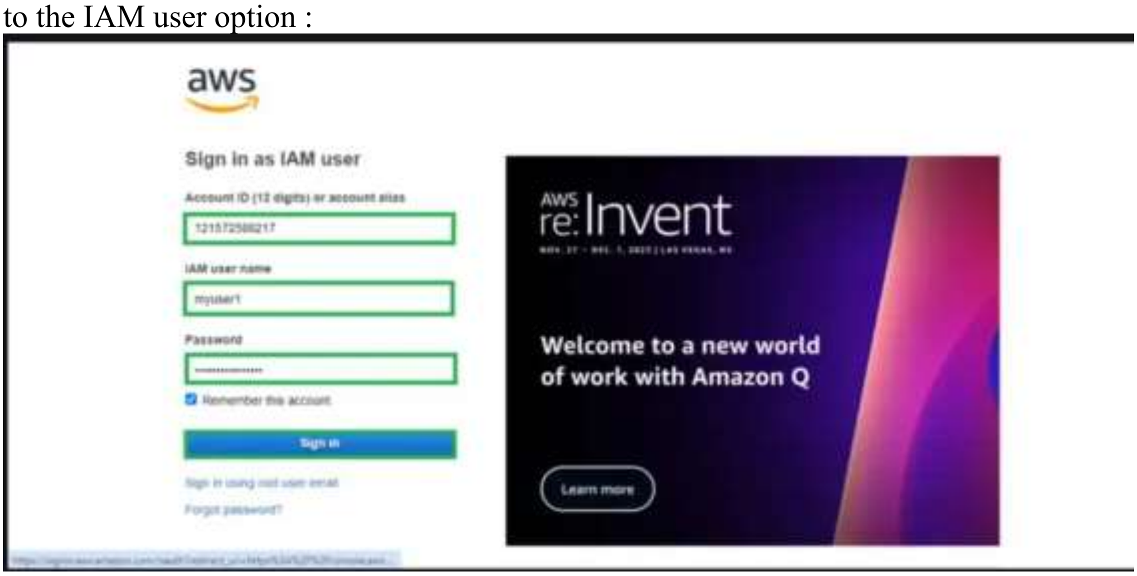
Step 7: **Login as IAM User**

- For logging in with the IAM user we need 3 things:

1. AWS account ID: You can get the AWS account Id by clicking the root user account in the right corner similar to the figure highlighted below.



2. IAM Username: The IAM user name that you created
3. Password: The password that you set for this IAM user
Fill in the asking details such as AWS account ID, IAM user, and Password from the sign-in portal going to the IAM user option :


Sign in as IAM user

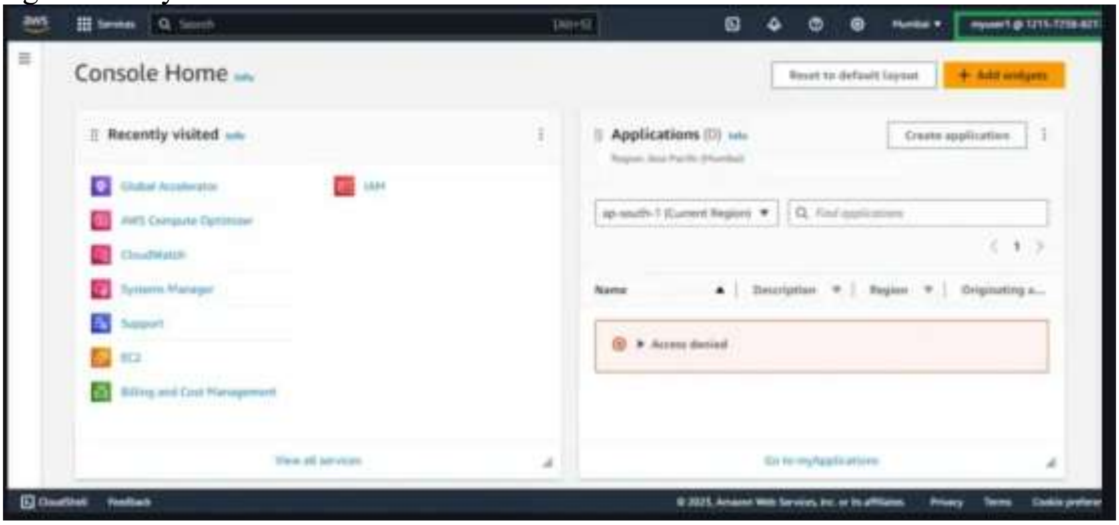
Account ID (12 digits) or account alias: 121572588217

IAM user name: myuser1

Password: ••••••••••••••••

☑ Remember this account

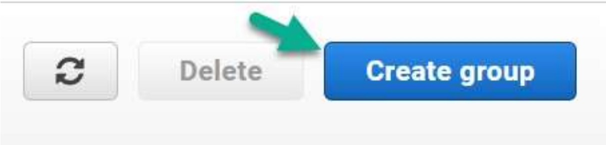
Once you log in successfully you can view the page link like this as shown below figure, on top of the right corner you can we see the IAM username with account ID:

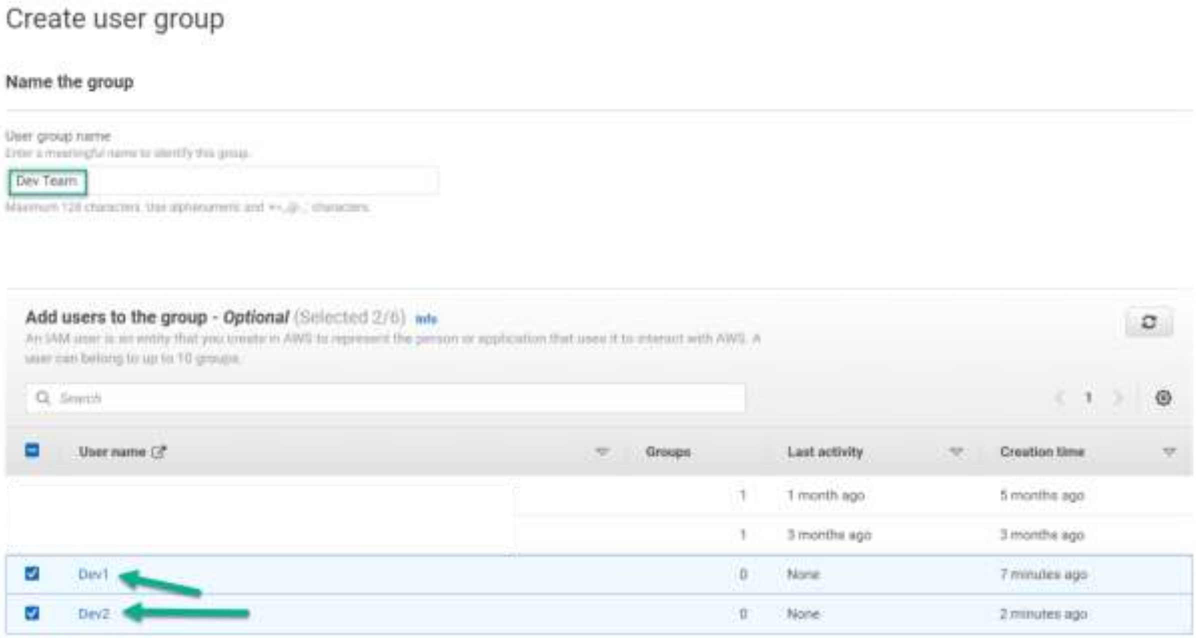


If you reached to this final interface then you performed the creation and login with the IAM user successfully**.**

Create Groups

IAM Console → Create Group





Create user group

Name the group

User group name
Enter a meaningful name to identify this group.

Dev Team

Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Add users to the group - ***Optional*** (Selected 2/6) Info

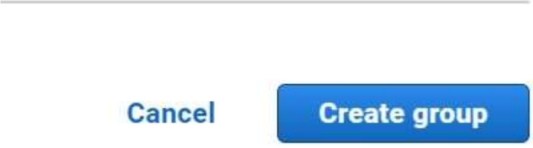
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS. A user can belong to up to 10 groups.

Search

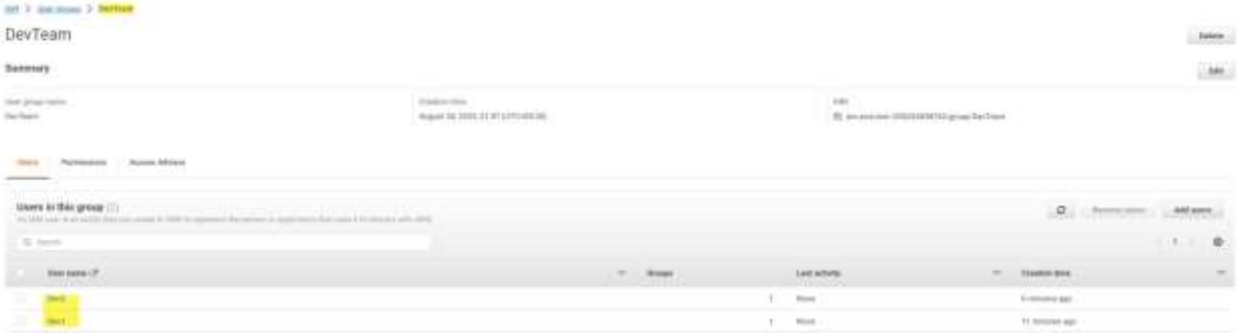
☐	User name	Groups	Last activity	Creation time
		1	1 month ago	5 months ago
		1	3 months ago	3 months ago
☑	Dev1	0	None	7 minutes ago
☑	Dev2	0	None	2 minutes ago

Provide Group Name as "DevTeam" (No Space)

Select Dev1 and Dev2 users to include them in the "Dev Team" group



Click on Create Group



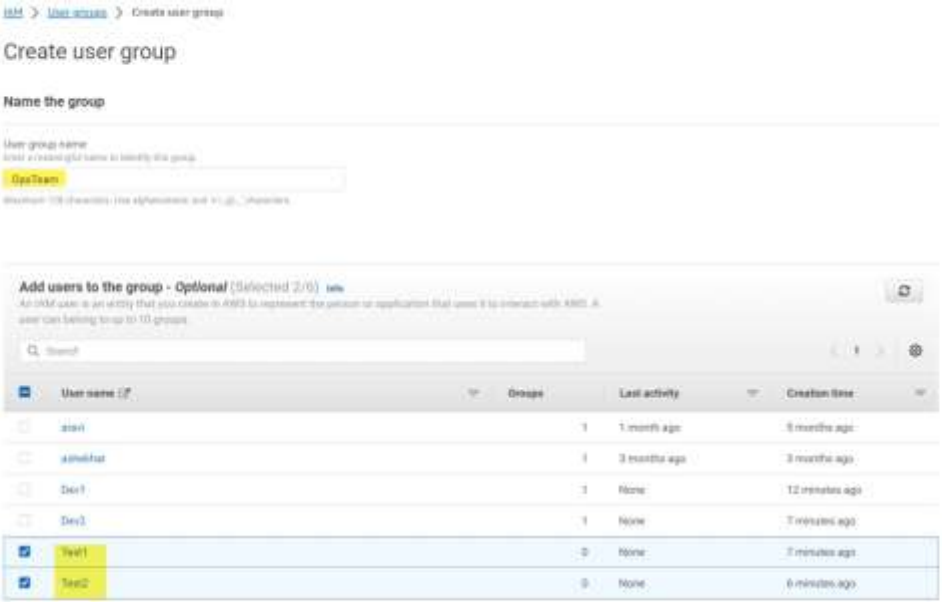
DevTeam

Summary

Users in this group

User name	Groups	Last activity	Creation time
Dev2	1	None	[illegible]
Dev1	1	None	[illegible]

That's it DevTeam group is completed, in similar way create OpsTeam



IAM > User groups > Create user group

Create user group

Name the group

User group name

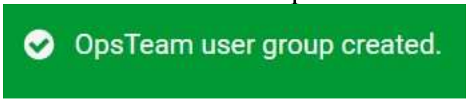
OpsTeam

Add users to the group - Optional (Selected 2/6) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS. A user can belong to up to 10 groups.

	User name	Groups	Last activity	Creation time
☐	aiani	1	1 month ago	5 months ago
☐	ashekhar	1	3 months ago	3 months ago
☐	Dev1	1	None	12 minutes ago
☐	Dev2	1	None	7 minutes ago
☑	Test1	0	None	7 minutes ago
☑	Test2	0	None	6 minutes ago

Click on “Create Group”



OpsTeam user group created.

OpsTeam

Done.

PRACTICAL-6

Aim: Creation of S3 Bucket and uploading files , S3 Static website hosting, S3 Replications

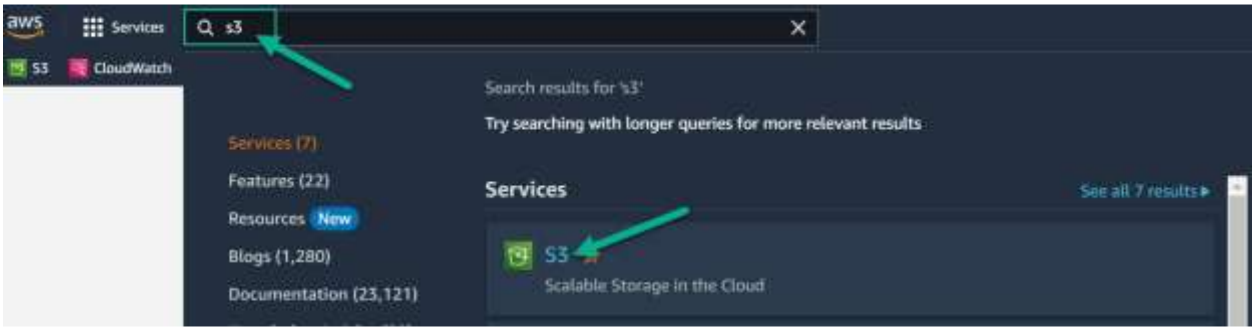
Tasks To Be Performed:

1. Create an S3 Bucket for file storage.

2. Upload 5 objects with different file extensions.

Answer:

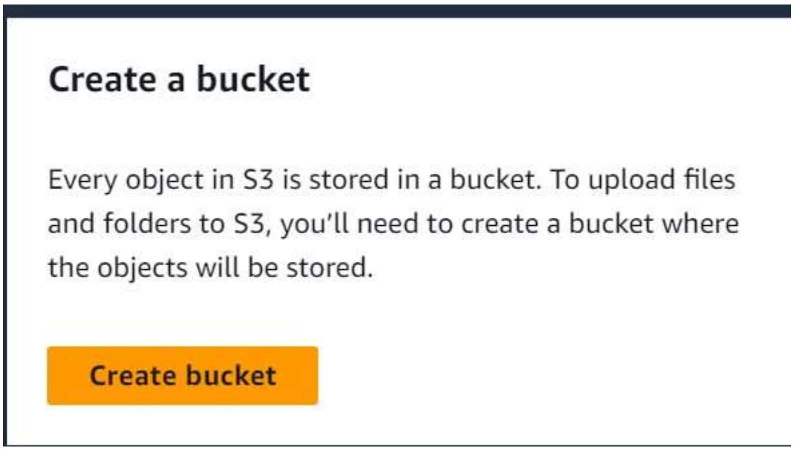
Login to the AWS Console providing your credentials



Search results for 's3'

Try searching with longer queries for more relevant results

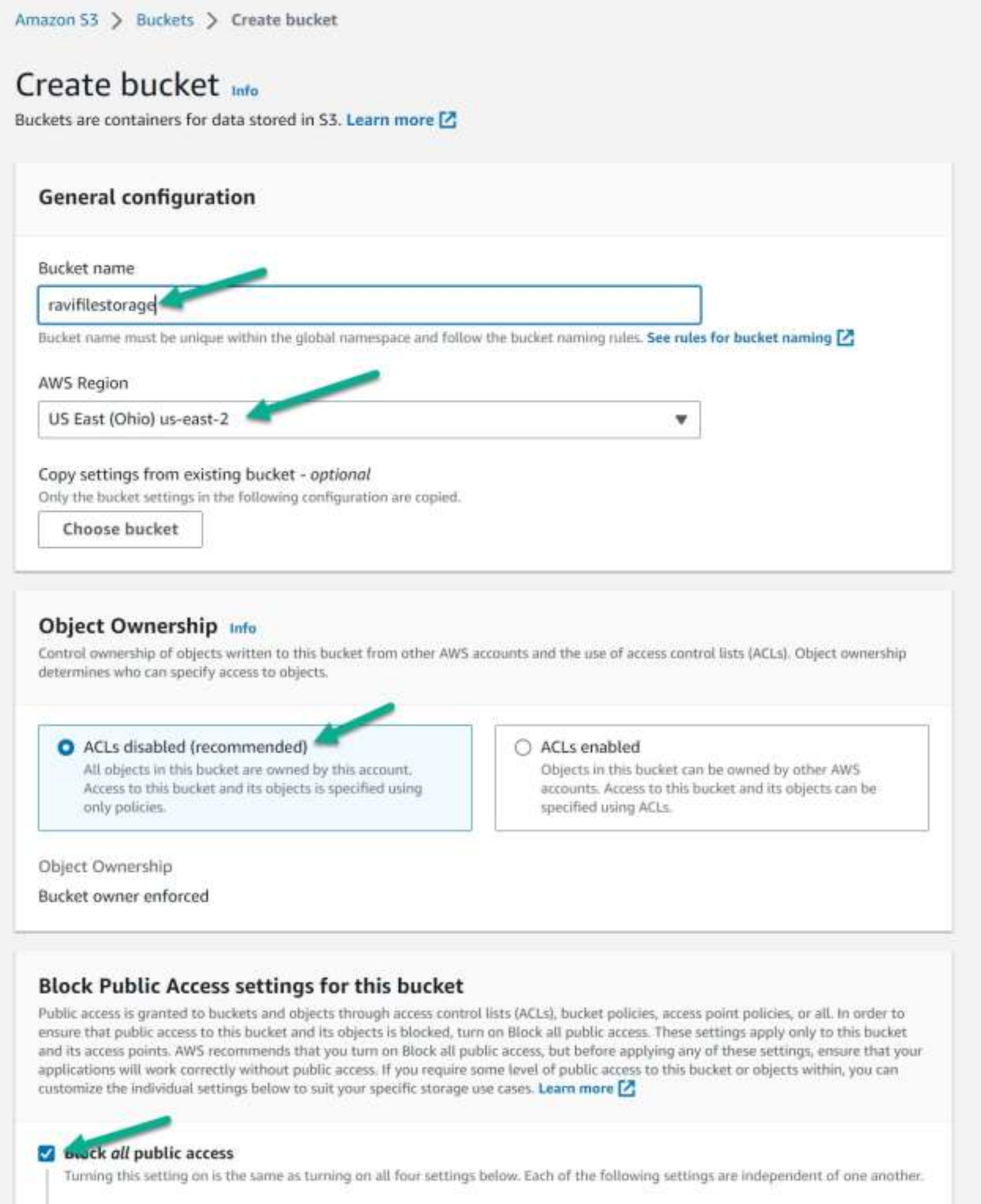
In Search bar search for S3 then select S3 in results



Create a bucket

Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

In S3 Console Click on "Create Bucket"



Create bucket Info

Buckets are containers for data stored in S3. Learn more

General configuration

Bucket name

ravifilestorage

Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

AWS Region

US East (Ohio) us-east-2

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

● ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

○ ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership

Bucket owner enforced

Block Public Access settings for this bucket

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 this bucket and its 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 this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

☑ Bck *all* public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

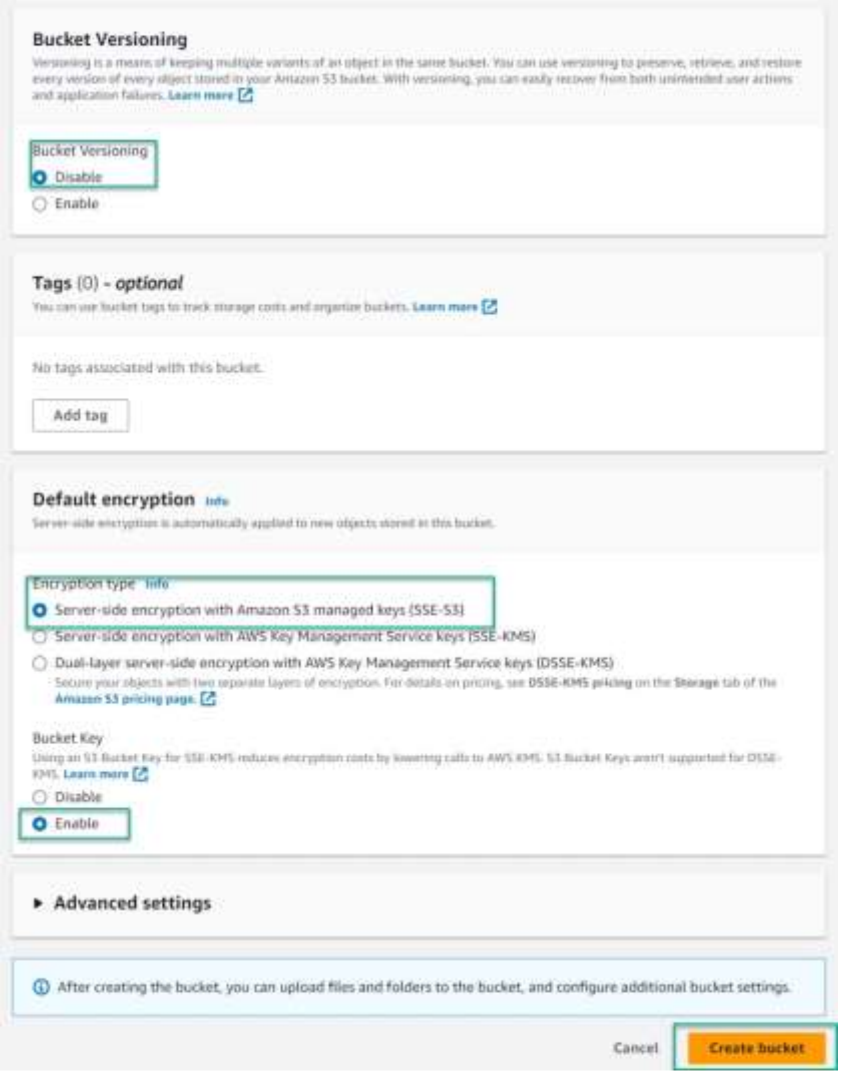
Provide Bucket Name should be unique

Select the region in which region you wanted to create that bucket

Object Ownership

ACLs Disabled

Select “Block All Public Access” to avoid publishing your bucket to public



Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

Bucket Versioning

● Disable

○ Enable

Tags (0) - *optional*

You can use bucket tags to track storage costs and organize buckets. Learn more

No tags associated with this bucket.

Default encryption Info

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type Info

● Server-side encryption with Amazon S3 managed keys (SSE-S3)

○ Server-side encryption with AWS Key Management Service keys (SSE-KMS)

○ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the Amazon S3 pricing page.

Bucket Key

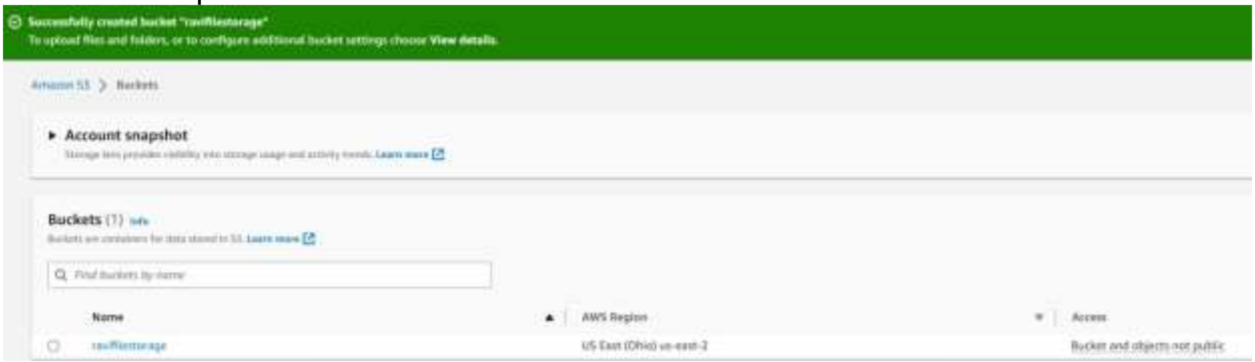
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more

○ Disable

● Enable

After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Keep all the Default options Click on “Create Bucket”



Successfully created bucket "ravifilestorage"
To upload files and folders, or to configure additional bucket settings choose View details.

Storage lens provides visibility into storage usage and activity trends. Learn more

Buckets (1) Info

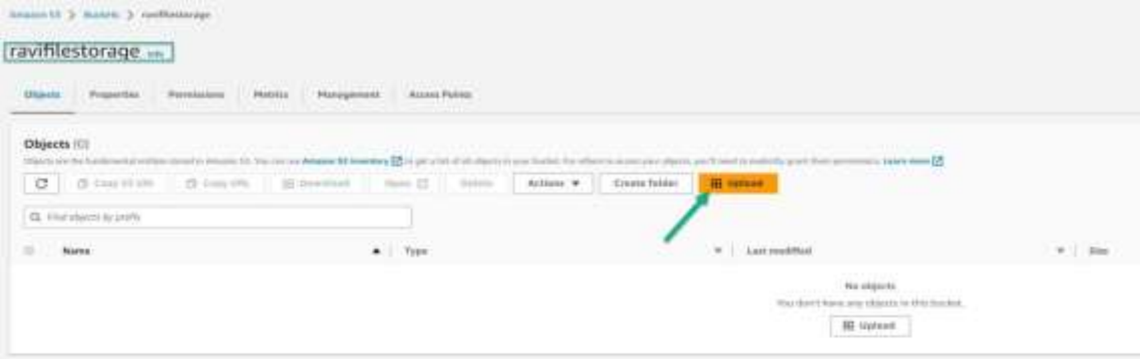
Buckets are containers for data stored in S3. Learn more

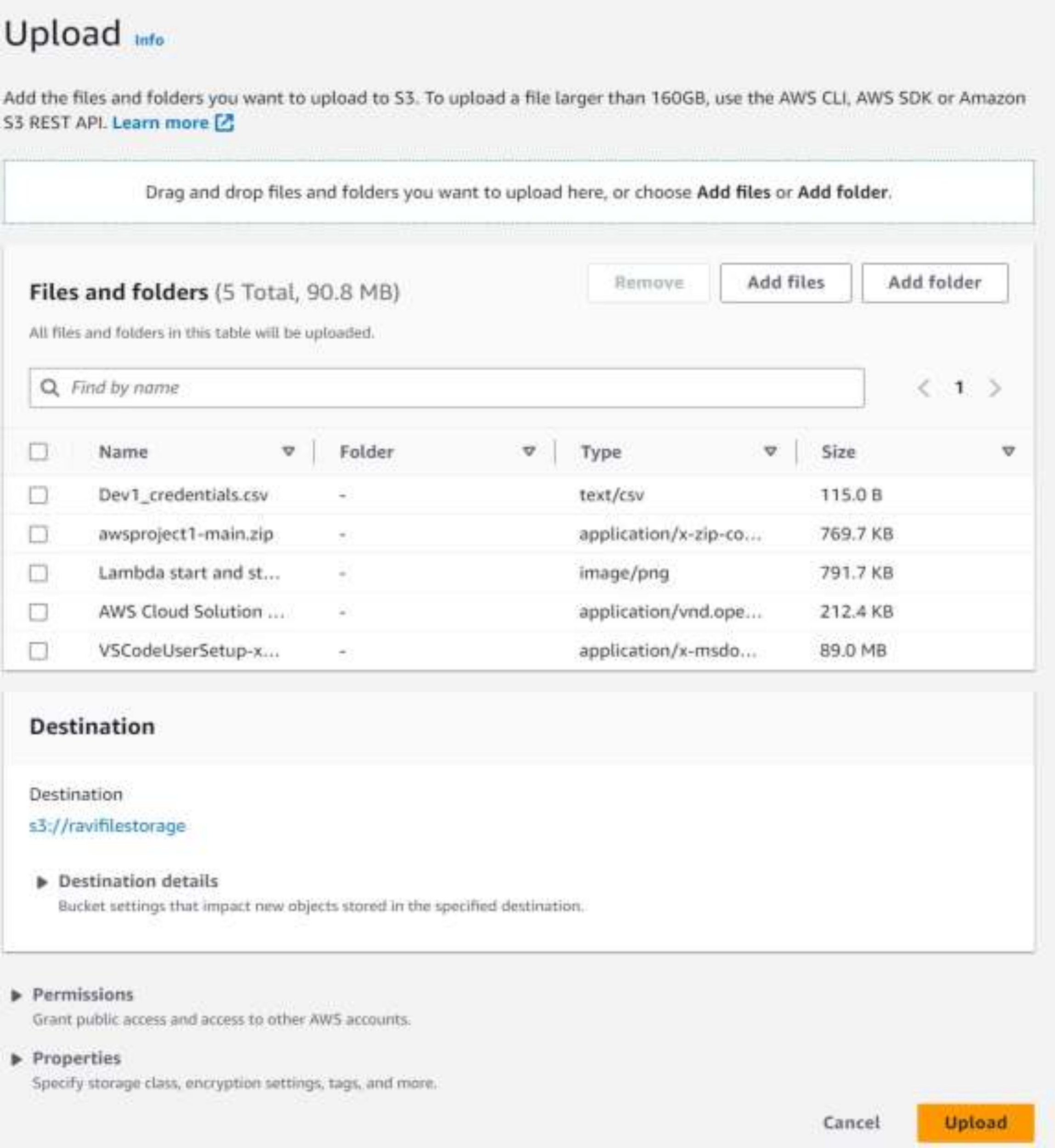
	Name	AWS Region	Access
○	ravifilestorage	US East (Ohio) us-east-2	Bucket and objects not public

Bucket is creation is successful

Now Upload the Files

Click on the Bucket Name → Click Upload





Upload Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more

Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

Files and folders (5 Total, 90.8 MB)

All files and folders in this table will be uploaded.

□	Name	Folder	Type	Size
□	Dev1_credentials.csv	-	text/csv	115.0 B
□	awsproject1-main.zip	-	application/x-zip-co...	769.7 KB
□	Lambda start and st...	-	image/png	791.7 KB
□	AWS Cloud Solution ...	-	application/vnd.ope...	212.4 KB
□	VSCodeUserSetup-x...	-	application/x-msdo...	89.0 MB

Destination

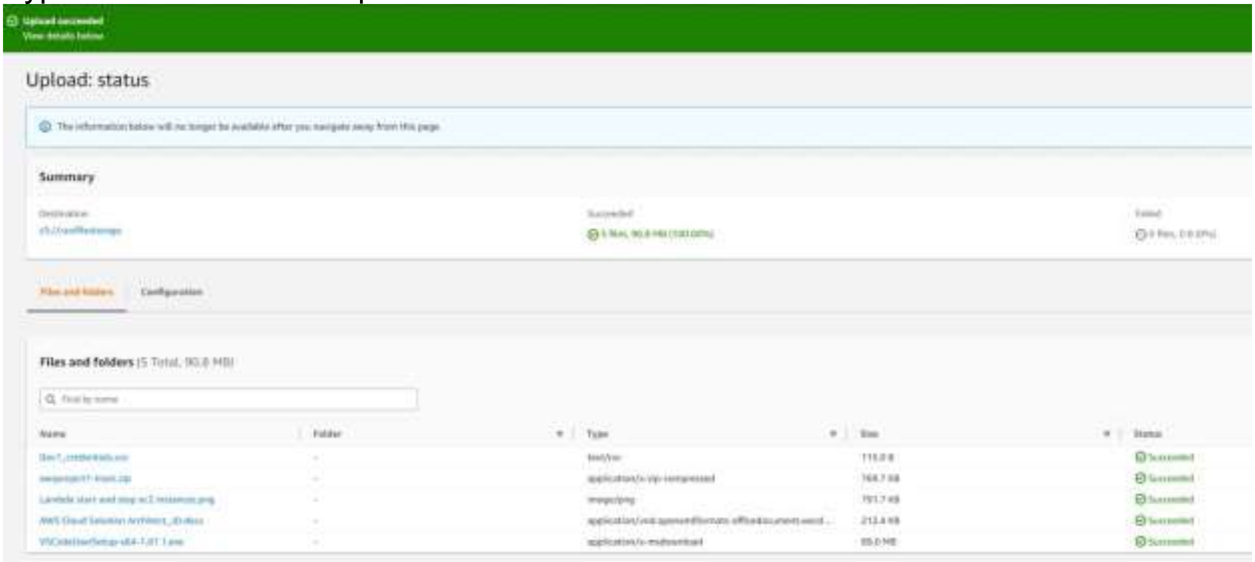
Destination
s3://ravifilestorage

▶ **Destination details**
Bucket settings that impact new objects stored in the specified destination.

▶ **Permissions**
Grant public access and access to other AWS accounts.

▶ **Properties**
Specify storage class, encryption settings, tags, and more.

Select 5 types of Files Click on Upload



Upload succeeded
View details below

Upload: status

The information below will no longer be available after you navigate away from this page

Summary

Destination: [illegible]

Succeeded: 5 files, 90.8 MB (100.00%)

Failed: 0 files, 0 B (0%)

Files and folders (5 Total, 90.8 MB)

Name	Folder	Type	Size	Status
[illegible]	-	text/csv	115.0 B	Succeeded
[illegible].zip	-	application/x-zip-compressed	168.7 KB	Succeeded
Lambda start and stop ec2 instances.png	-	image/png	751.7 KB	Succeeded
AWS Cloud Solution Architect_ID.docx	-	application/vnd.openxmlformats-officedocument.word...	213.4 KB	Succeeded
VSCodeUserSetup-x64-[illegible].exe	-	application/x-msdownload	[illegible] MB	Succeeded

Files are uploaded successfully .

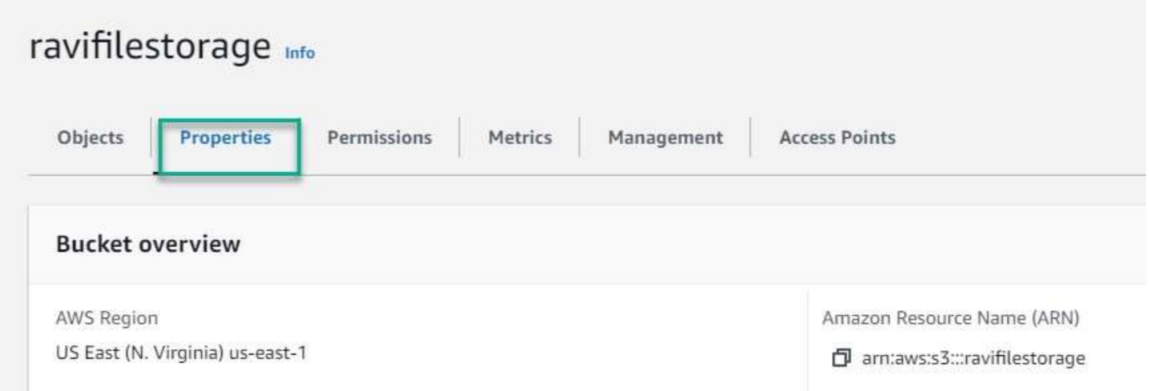
S3 Static website hosting

Tasks to Be Performed:

1. Use the created bucket in the previous task to host static websites, and upload an index.html file and error.html page.

Answer

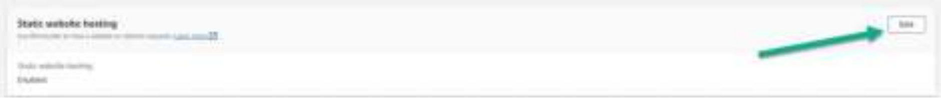
Now select the bucket you want to use for creating a static website, Click on Properties



Bucket overview

AWS Region
US East (N. Virginia) us-east-1

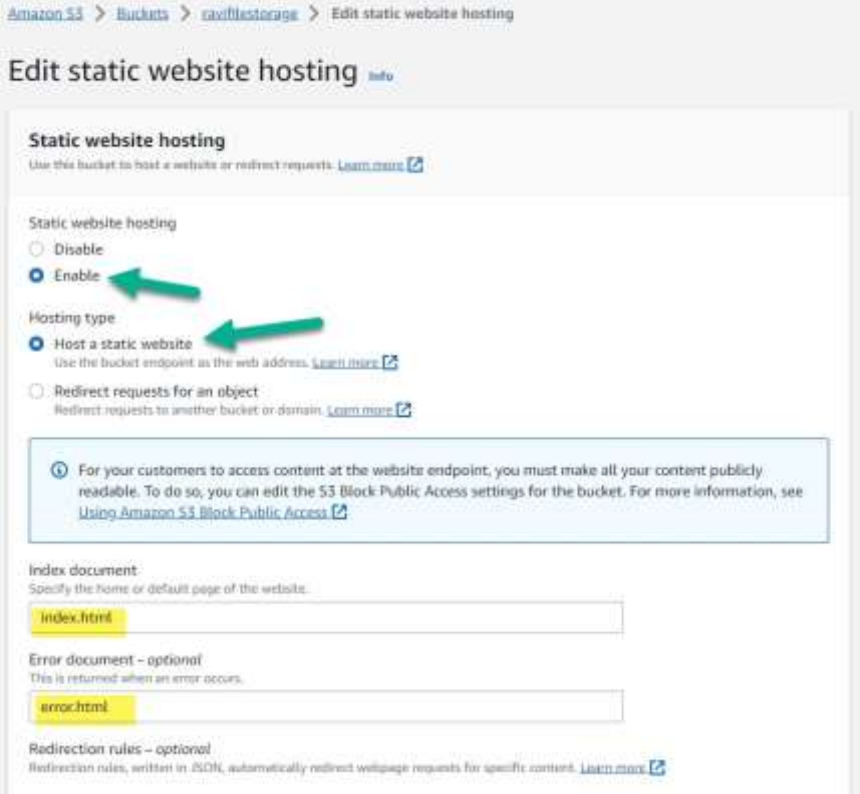
Amazon Resource Name (ARN)
arn:aws:s3:::ravifilestorage



Static website hosting
Use this bucket to host a website or redirect requests. Learn more

Static website hosting
Disabled

Edit the **Static Website hosting**


Amazon S3 > Buckets > ravifilestorage > Edit static website hosting
Info
Learn more

Edit static website hosting

Static website hosting
Use this bucket to host a website or redirect requests.

Static website hosting
○ Disable
● Enable

Hosting type
● Host a static website
Use the bucket endpoint as the web address.
○ Redirect requests for an object
Redirect requests to another bucket or domain.

For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see Using Amazon S3 Block Public Access

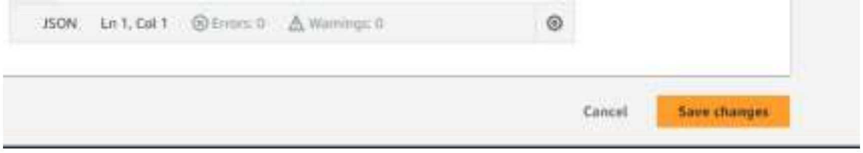
Index document
Specify the home or default page of the website.
index.html

Error document – *optional*
This is returned when an error occurs.
error.html

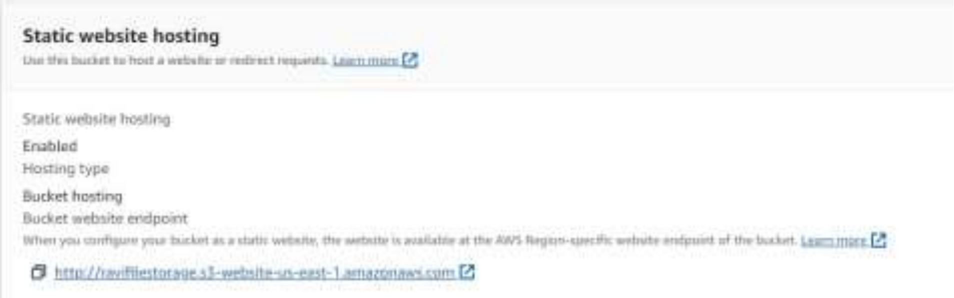
Redirection rules – *optional*
Redirection rules, written in JSON, automatically redirect webpage requests for specific content. Learn more

Select Enable

Provide the index.html and error.html file name they should be case sensitive and name should be matching as per the apache default configuration



Click “**Save Changes**”



Static website hosting

Use this bucket to host a website or redirect requests. Learn more

Static website hosting

Enabled

Hosting type

Bucket hosting

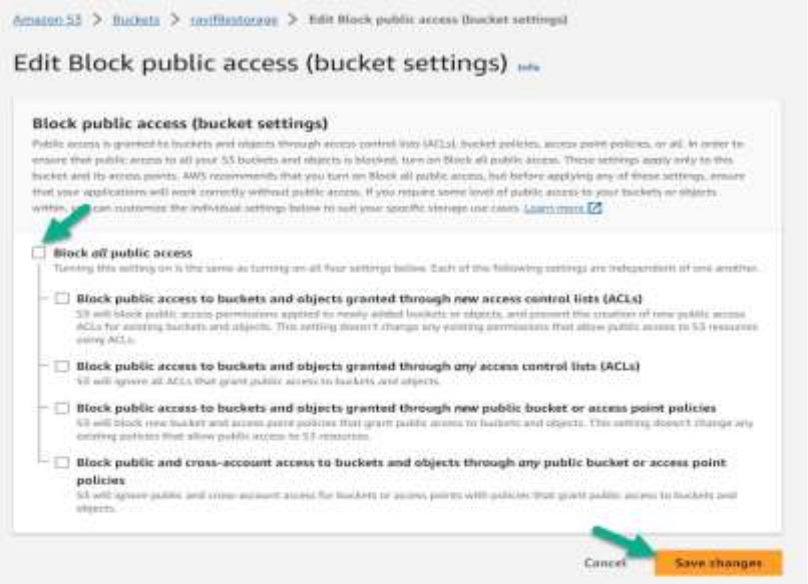
Bucket website endpoint

When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. Learn more

http://ravifilestorage.s3-website-us-east-1.amazonaws.com

http://ravifilestorage.s3-website-us-east-1.amazonaws.com
Once the website is enable it will provide you the endpoint details, you have to copy the URL and then browse is using the browser.

Before that, you have to upload index.html and error.html to the S3 bucket.



Amazon S3 > Buckets > ravifilestorage > Edit Block public access (bucket settings)

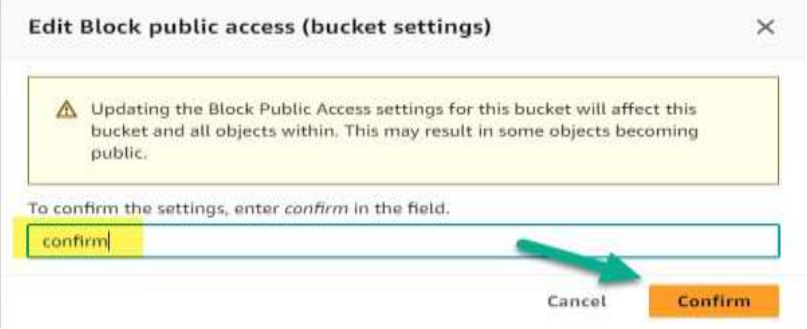
Edit Block public access (bucket settings) Info

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**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- □ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
  S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- □ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
  S3 will ignore all ACLs that grant public access to buckets and objects.
- □ **Block public access to buckets and objects granted through *new* public bucket or access point policies**
  S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- □ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
  S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.



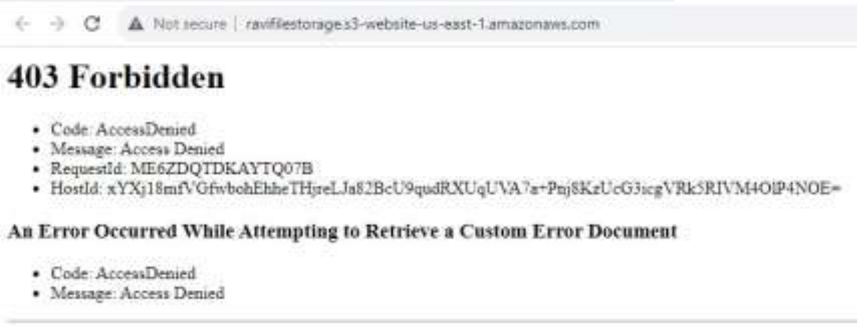
Edit Block public access (bucket settings)

Updating the Block Public Access settings for this bucket will affect this bucket and all objects within. This may result in some objects becoming public.

To confirm the settings, enter *confirm* in the field.

confirm

Once your enable the public access on the S3 bucket, you need to write the bucket policy otherwise it will give the below error message.



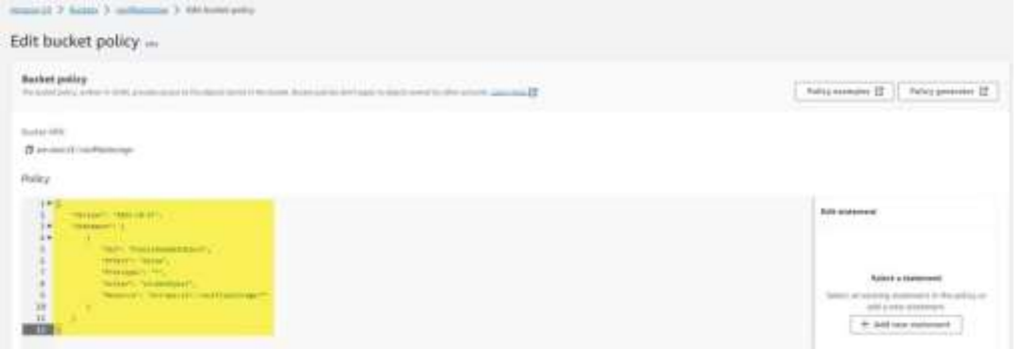
Not secure | ravifilestorage.s3-website-us-east-1.amazonaws.com

403 Forbidden

- Code: AccessDenied
- Message: Access Denied
- RequestId: ME6ZDQTDKAYTQ07B
- HostId: xYXj18mfVGfwbohEhheTHjreLJa82BcU9qudRXUqUVA7a+Pnj8KzUcG3icgVRk5RIVM4OlP4NOE=

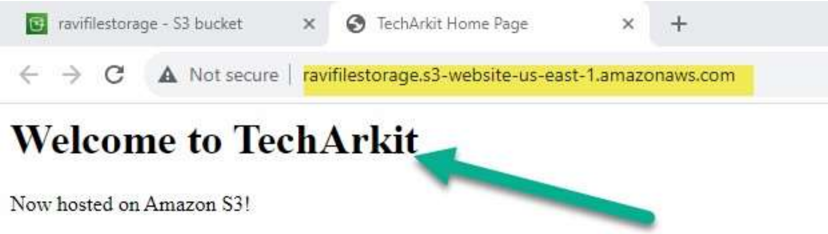
An Error Occurred While Attempting to Retrieve a Custom Error Document

- Code: AccessDenied
- Message: Access Denied



```
{
      "Version": "2012-10-17",
      "Statement": [
            {
                  "Sid": "PublicReadGetObject",
                  "Effect": "Allow",
                  "Principal": "*",
                  "Action": "s3:GetObject",
                  "Resource": "arn:aws:s3:::ravifilestorage/*"
            }
      ]
}
```

Add the bucket policy as shown above that's it your static website is published successfully.



Not secure | ravifilestorage.s3-website-us-east-1.amazonaws.com

Welcome to TechArkit

Now hosted on Amazon S3!

PRACTICAL_-7

Aim: Creation of VPC

Problem Statement:

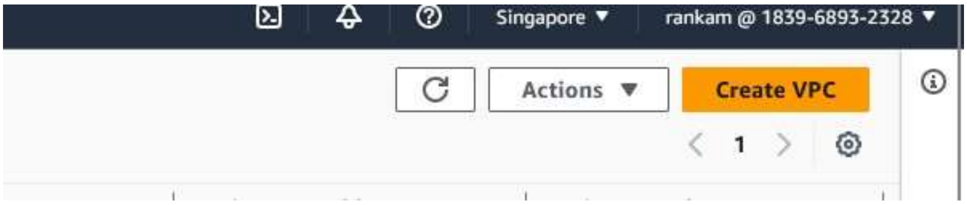
Working for an organization, you are required to provide them with a safe and secure environment for the deployment of their resources. They might require different types of connectivity. Implement the following to fulfill the requirements of the company.

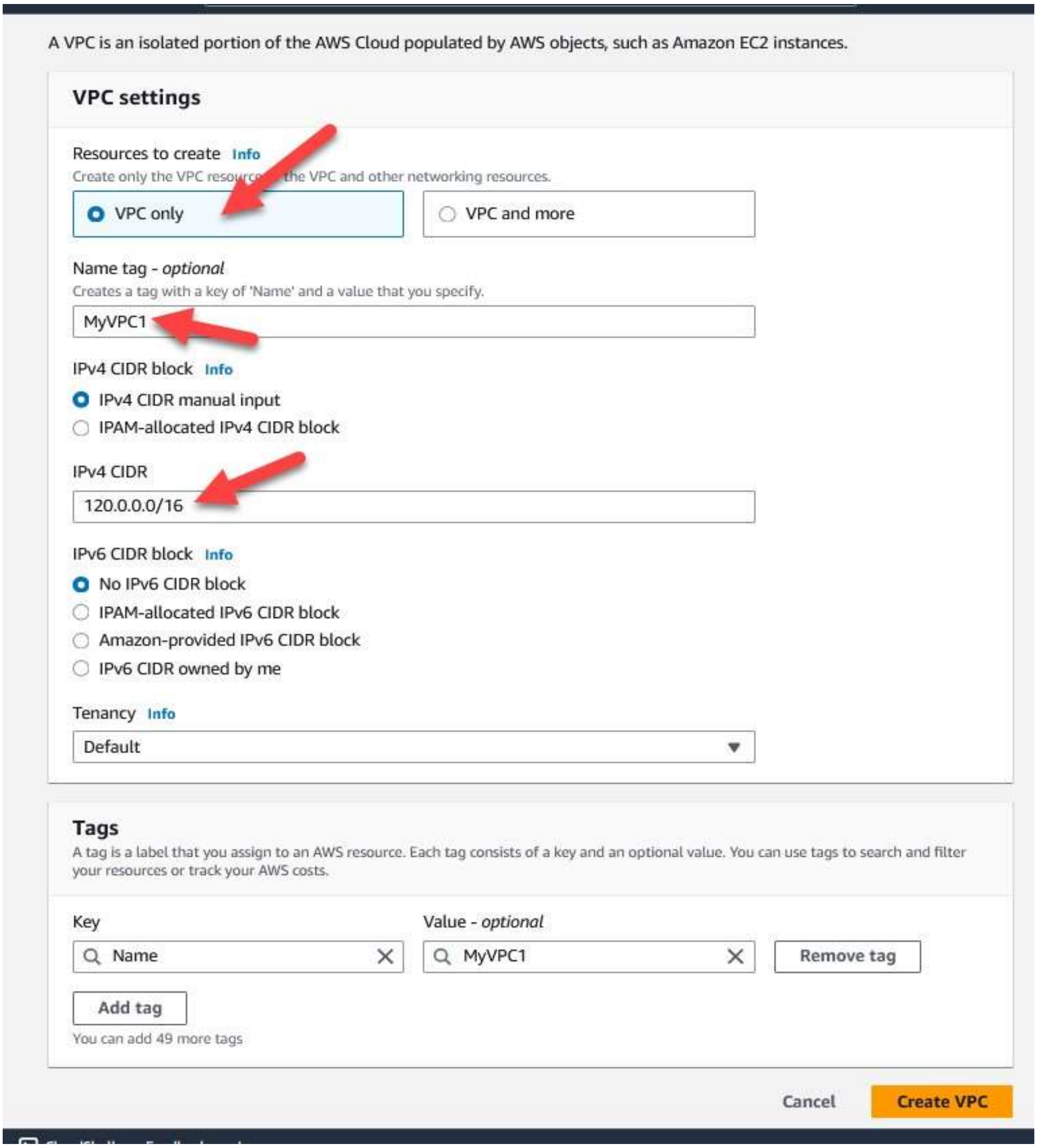
Tasks To Be Performed:

1. Create a VPC with 120.0.0.0/16 CIDR block.
2. Create 1 public subnet and 2 private subnets and make sure you connect a NAT gateway for internet connectivity to a private subnet

Answer:

Login to the AWS Management console
Services select **VPC → Create VPC**





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

VPC settings

Resources to create Info
Create only the VPC resource or the VPC and other networking resources.

● VPC only ○ VPC and more

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.
MyVPC1

IPv4 CIDR block Info
● IPv4 CIDR manual input
○ IPAM-allocated IPv4 CIDR block

IPv4 CIDR
120.0.0.0/16

IPv6 CIDR block Info
● No IPv6 CIDR block
○ IPAM-allocated IPv6 CIDR block
○ Amazon-provided IPv6 CIDR block
○ IPv6 CIDR owned by me

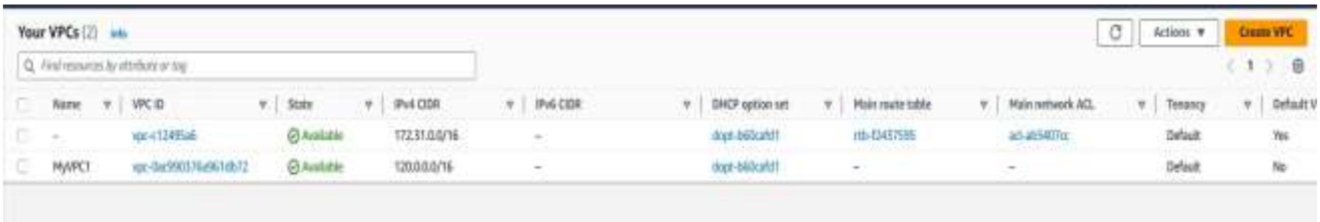
Tenancy Info
Default

Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key: Name
Value - *optional*: MyVPC1

1. Select VPC Only option to create VPC with customized options
2. Provide a VPC name
3. Select IPv4 CIDR manual input (Currently we are targeting for IPv4 only)
4. Select Default tenancy (Shared resources)

Click “Create VPC”



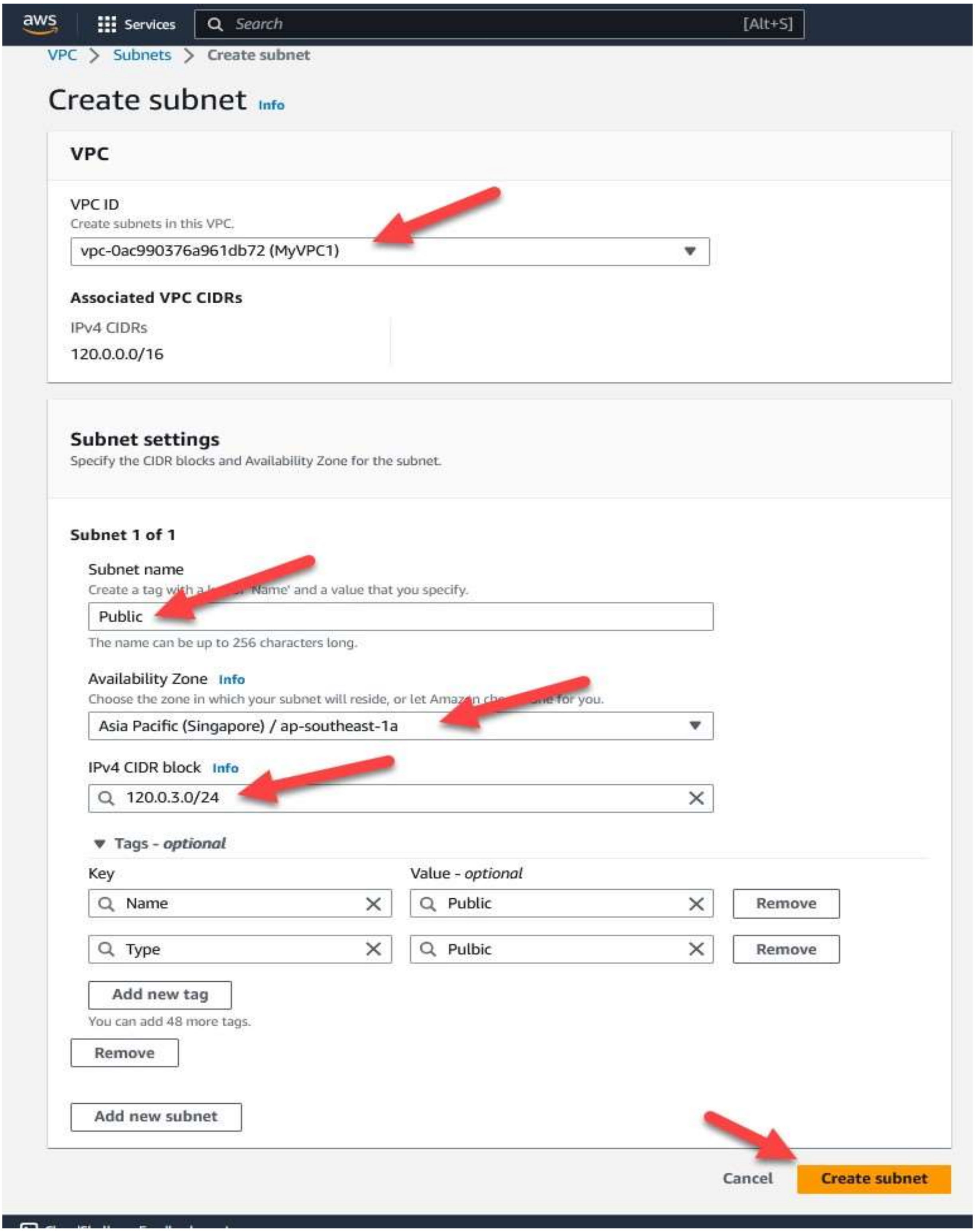
Your VPCs (2) Info

	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set	Main route table	Main network ACL	Tenancy	Default V
□	-	vpc-c12495a6	Available	172.31.0.0/16	-	dopt-b60cafd1	rtb-f2437595	acl-ab5407cc	Default	Yes
□	MyVPC1	vpc-0ae990376a961db72	Available	120.0.0.0/16	-	dopt-b60cafd1	-	-	Default	No

MyVPC1 is created successfully. Now create the subnets as per the requirement.

Creating Subnets

In VPC service → Click on subnets → Create subnet



VPC > Subnets > Create subnet

Create subnet Info

VPC

VPC ID
Create subnets in this VPC.
vpc-0ac990376a961db72 (MyVPC1)

Associated VPC CIDRs

IPv4 CIDRs
120.0.0.0/16

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
Public
The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
Asia Pacific (Singapore) / ap-southeast-1a

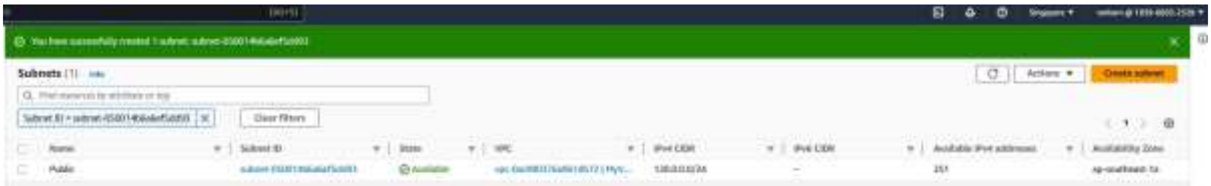
IPv4 CIDR block Info
120.0.3.0/24

▼ Tags - *optional*

Key	Value - *optional*	
Name	Public	Remove
Type	Pulbic	Remove

1. Select the correct VPC.
2. Provide a subnet Name i.e., Public
3. Assign the IPv4 CIDR block for this subnet 120.0.3.0/24.
4. Provide Tags for easy tracking and identification.

Click “Create subnet”



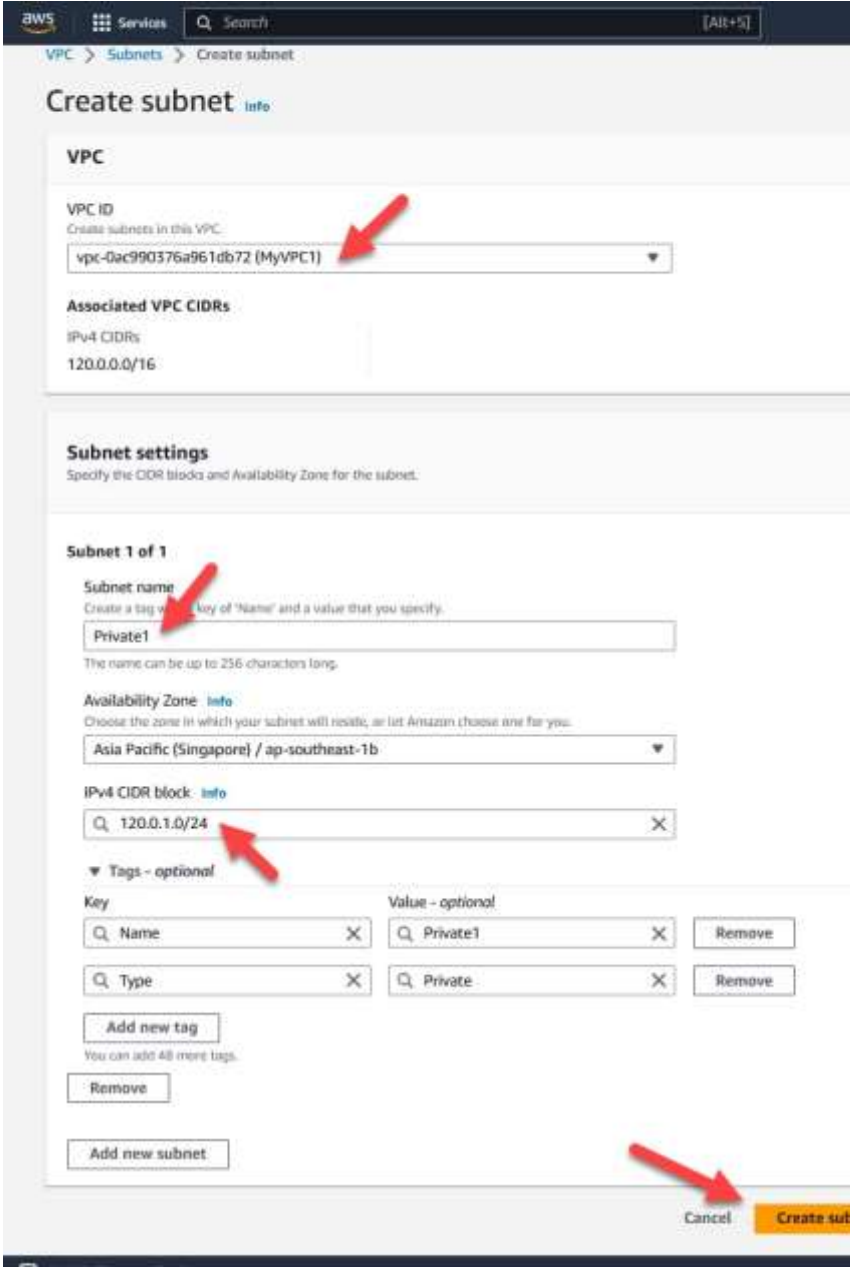
You have successfully created 1 subnet: subnet-050014[illegible]

Subnets (1) Info

Subnet ID = subnet-050014[illegible]

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses	Availability Zone
Public	subnet-050014[illegible]	Available	vpc-0ac990376a961db72 | MyV...	120.0.0.0/24	–	251	ap-southeast-1a

The public subnet has been created successfully.



Create subnet Info

VPC

VPC ID
Create subnets in this VPC.
vpc-0ac990376a961db72 (MyVPC1)

Associated VPC CIDRs
IPv4 CIDRs
120.0.0.0/16

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
Private1
The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
Asia Pacific (Singapore) / ap-southeast-1b

IPv4 CIDR block Info
120.0.1.0/24

Tags - optional

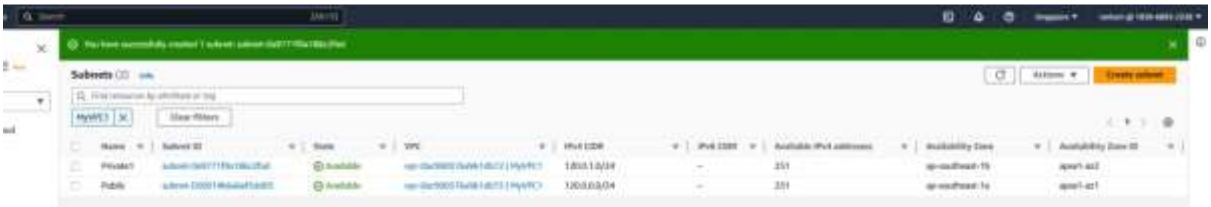
Key	Value - optional
Name	Private1
Type	Private

You can add 48 more tags.

Click“**Create subnet**”

1. Select the appropriate VPC.
2. Provide a subnet name i.e., Private1.
3. Select the AZ (Availability Zone) and select a different AZ than another subnet for redundancy.
4. Provide IPv4 CIDR block i.e., 120.0.1.0/24.

Click“**Create subnet**”



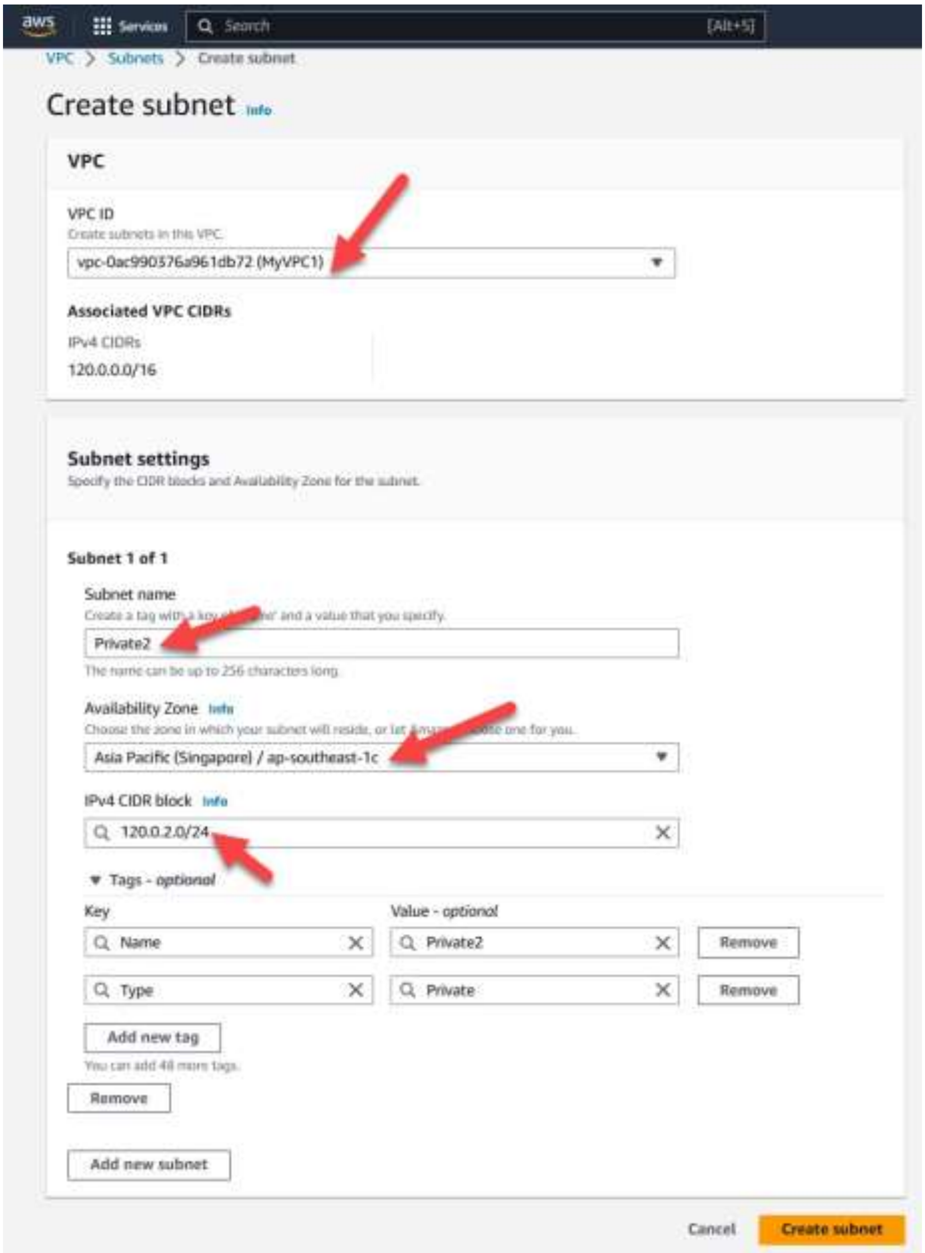
You have successfully created 1 subnet: subnet-[illegible]

Subnets (2)

MyVPC1

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses	Availability Zone	Availability Zone ID
Private1	subnet-[illegible]	Available	vpc-0ac990376a961db72 | MyVPC1	120.0.1.0/24	–	251	ap-southeast-1b	apse1-az2
Public	subnet-[illegible]	Available	vpc-0ac990376a961db72 | MyVPC1	120.0.0.0/24	–	251	ap-southeast-1a	apse1-az1

Private1 subnet created successfully.



Create subnet

VPC

VPC ID
Create subnets in this VPC.
vpc-0ac990376a961db72 (MyVPC1)

Associated VPC CIDRs
IPv4 CIDRs
120.0.0.0/16

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
Private2
The name can be up to 256 characters long.

Availability Zone
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
Asia Pacific (Singapore) / ap-southeast-1c

IPv4 CIDR block
120.0.2.0/24

Tags - optional

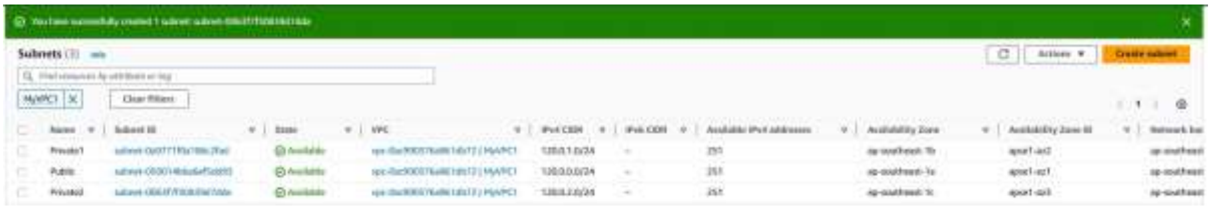
Key	Value - optional
Name	Private2
Type	Private

You can add 48 more tags.

Click Create subnet

1. Select appropriate VPC,
2. Provide a subnet name i.e., Private2.
3. Select the AZ (Availability Zone) and select a different AZ than another subnet for redundancy.

4. Provide IPv4 CIDR block i.e., 120.0.2.0/24.
Click“**Create subnet**”

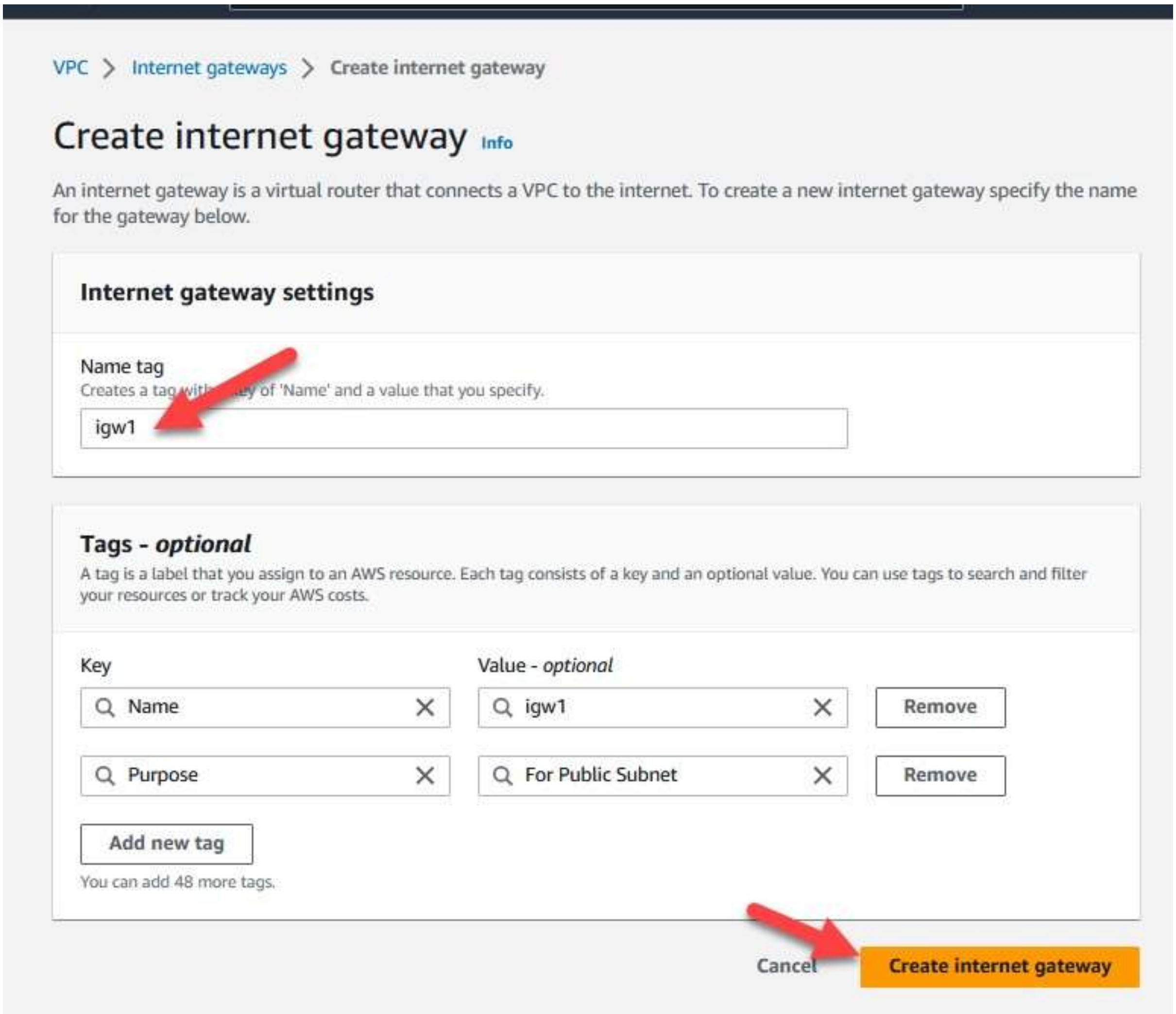


You have successfully created 1 subnet: subnet-[illegible]

Subnets (3)

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses	Availability Zone	Availability Zone ID	Network bo
Private1	[illegible]	Available	[illegible] | MyVPC1	120.0.1.0/24	–	251	ap-southeast-1b	apse1-az2	ap-southeast
Public	[illegible]	Available	[illegible] | MyVPC1	120.0.0.0/24	–	251	ap-southeast-1a	apse1-az1	ap-southeast
Private2	[illegible]	Available	[illegible] | MyVPC1	120.0.2.0/24	–	251	ap-southeast-1c	apse1-az3	ap-southeast

Create Internet Gateway



VPC > Internet gateways > Create internet gateway

Create internet gateway Info

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag
Creates a tag with a key of 'Name' and a value that you specify.
igw1

Tags - *optional*
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*
Name	igw1
Purpose	For Public Subnet

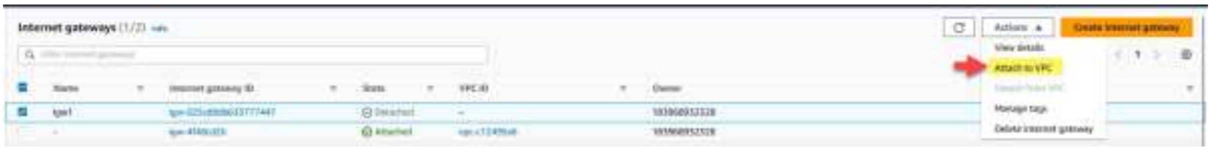
You can add 48 more tags.

Click on “Create Internet Gateway”

a. Provide a Internet Gateway a Name “**igw1**”
b. Provide Tags for later identification

Click “**Create internet Gateway**” IGW is

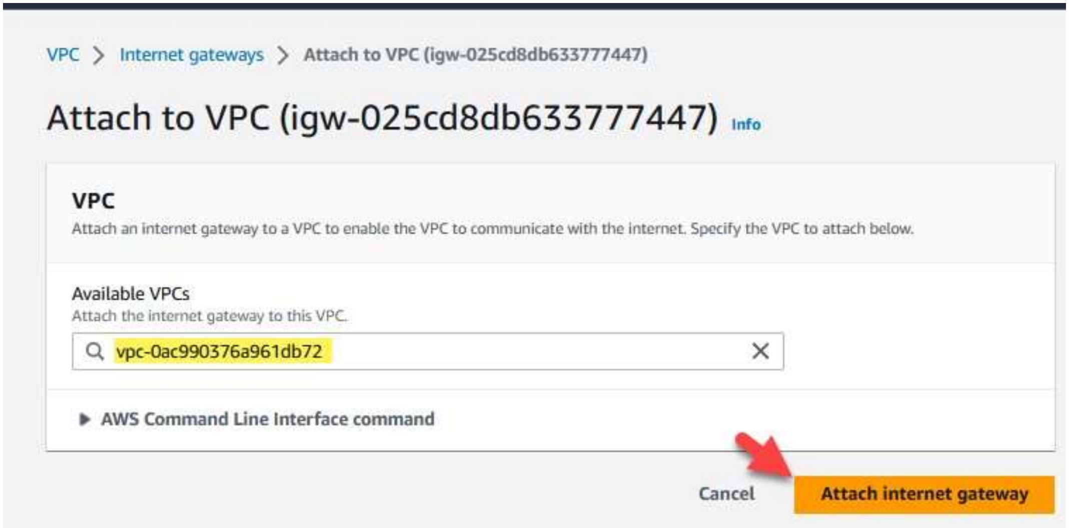
created successfully.



Internet gateways (1/2) Info

Name	Internet gateway ID	State	VPC ID	Owner
igw1	igw-025cd8db633777447	Detached	–	103968932328
–	igw-4146c2c5	Attached	vpc-c12495a8	103968932328

Select the “igw1” which is newly created, **Actions → Attach to VPC**



VPC > Internet gateways > Attach to VPC (igw-025cd8db633777447)

Attach to VPC (igw-025cd8db633777447) Info

VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs

Attach the internet gateway to this VPC.

vpc-0ac990376a961db72

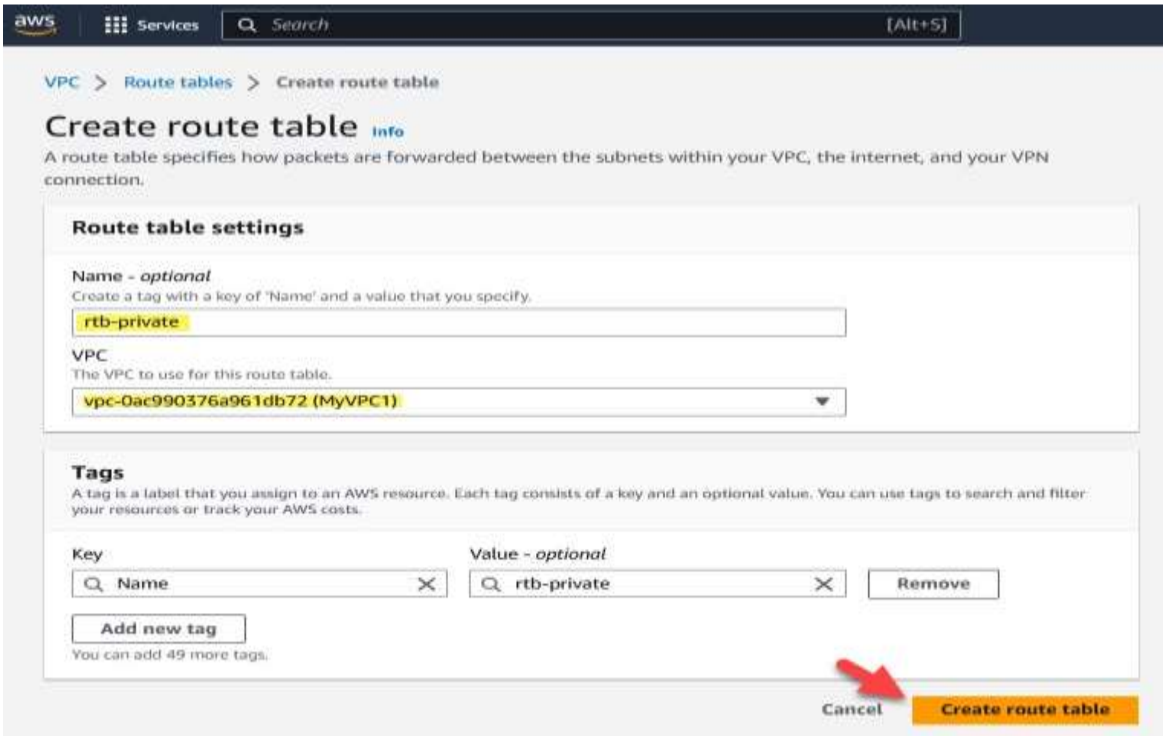
Select “MyVPC1” which is a newly created then click on “**Attach internet gateway**”

Enable Internet Route to Public Subnet

We require multiple route tables to add routes to them. Since we have a single route table I am going to create another route table for the private subnet.

1. De-associate private subnets from existing subnets (to avoid having IGW and route table)
2. Associate private subnets to the “rtb-private” subnet to have different routes.

In VPC service → route tables → Create route table



VPC > Route tables > Create route table

Create route table Info

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - *optional*

Create a tag with a key of 'Name' and a value that you specify.

rtb-private

VPC

The VPC to use for this route table.

vpc-0ac990376a961db72 (MyVPC1)

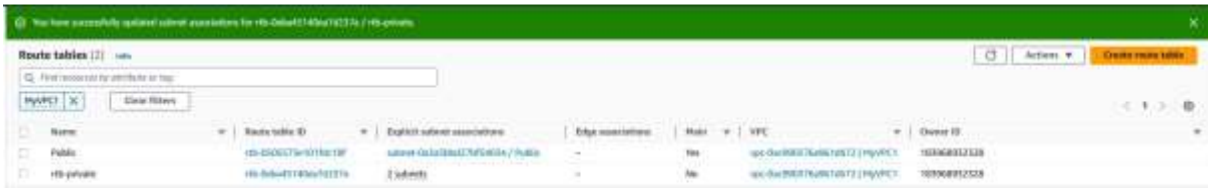
Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*
Name	rtb-private

You can add 49 more tags.

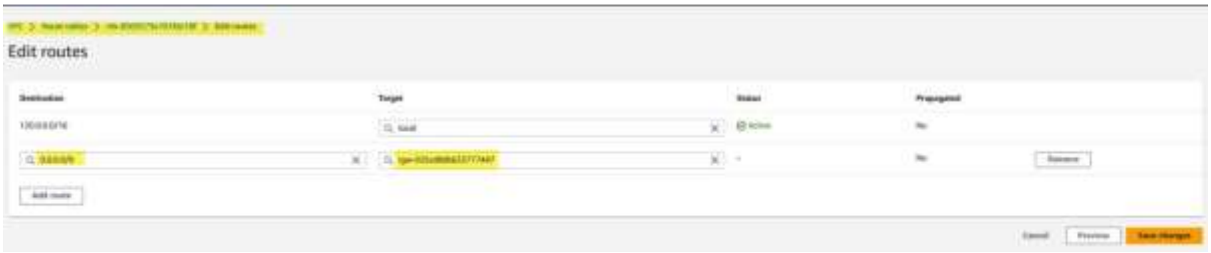
Click“**Create route table**”



Route tables (2)

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC	Owner ID
Public	[illegible]	[illegible] / Public	–	Yes	[illegible] | MyVPC1	[illegible]
rtb-private	[illegible]	2 subnets	–	No	[illegible] | MyVPC1	[illegible]

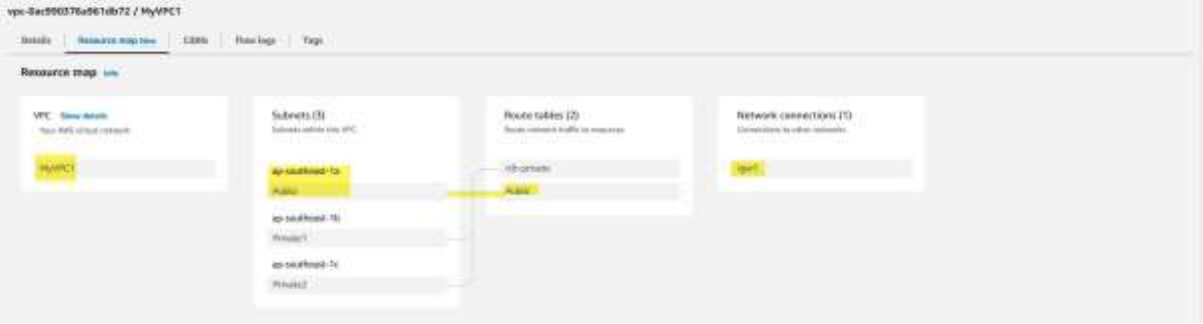
Edit Public route table and add internet route



Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-[illegible]	-	No

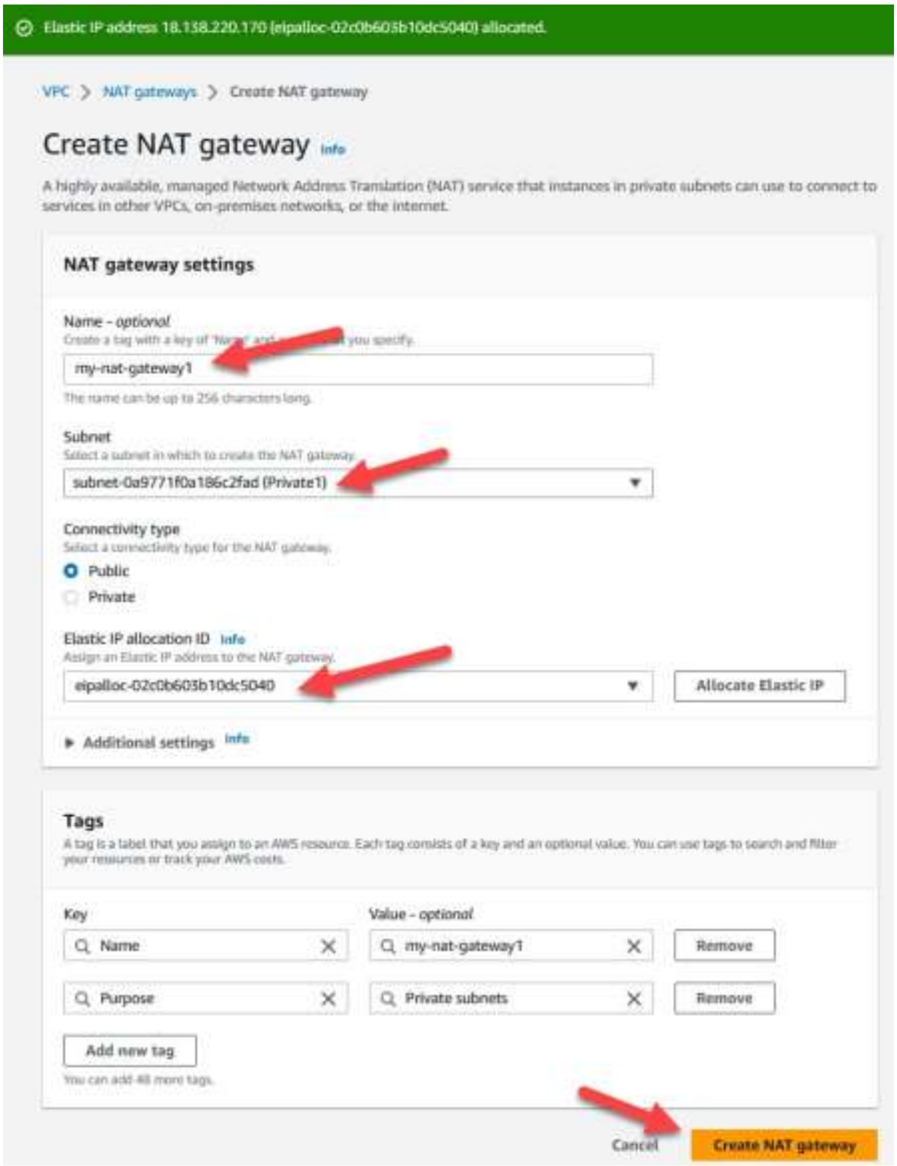
Now Public subnet have internet access.



vpc-0ac900376a961db72 / MyVPC1

Create NAT Gateway

VPC Service → NAT gateways → Create NAT gateways →



Elastic IP address 18.138.220.170 (eipalloc-02c0b603b10dc5040) allocated.

VPC > NAT gateways > Create NAT gateway

Create NAT gateway Info

A highly available, managed Network Address Translation (NAT) service that instances in private subnets can use to connect to services in other VPCs, on-premises networks, or the internet.

NAT gateway settings

Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.
my-nat-gateway1
The name can be up to 256 characters long.

Subnet
Select a subnet in which to create the NAT gateway.
subnet-0a9771f0a186c2fad (Private1)

Connectivity type
Select a connectivity type for the NAT gateway.
● Public
○ Private

Elastic IP allocation ID Info
Assign an Elastic IP address to the NAT gateway.
eipalloc-02c0b603b10dc5040

Tags

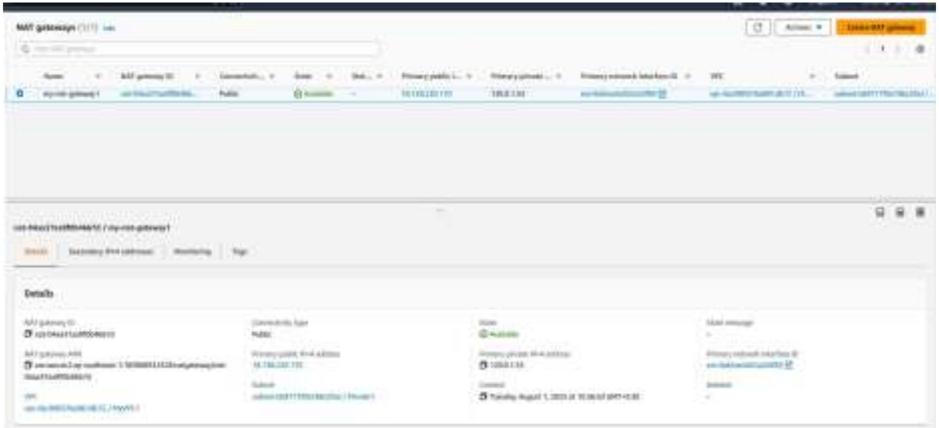
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*
Name	my-nat-gateway1
Purpose	Private subnets

You can add 48 more tags.

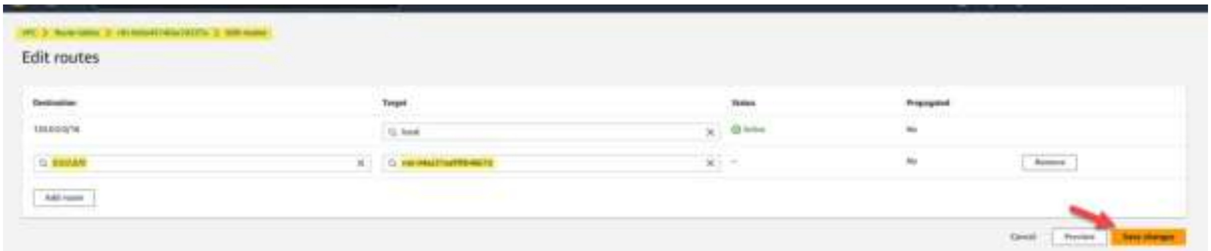
a. Provide a NAT gateway name i.e., my-nat-gateway1.
b. Select the subnets.
c. Connectivity type Public
d. Assign Elastic IP

Click “Create NAT Gateway”



NAT Gateway is created successfully.

VPC Service → Route tables → Select Private route table → Edit route table



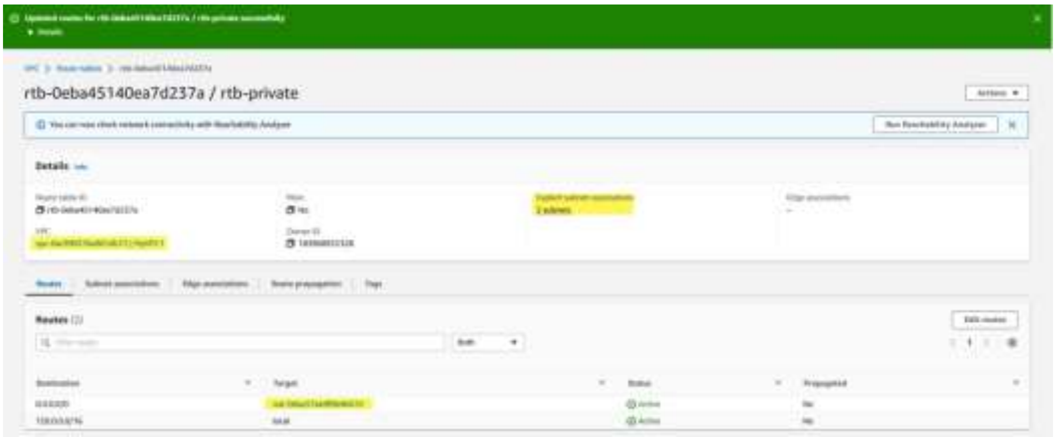
Edit routes

Add another route

Destination: 0.0.0.0/0

Target: NAT-GATEWAY

Click “Save Changes”



rtb-0eba45140ea7d237a / rtb-private

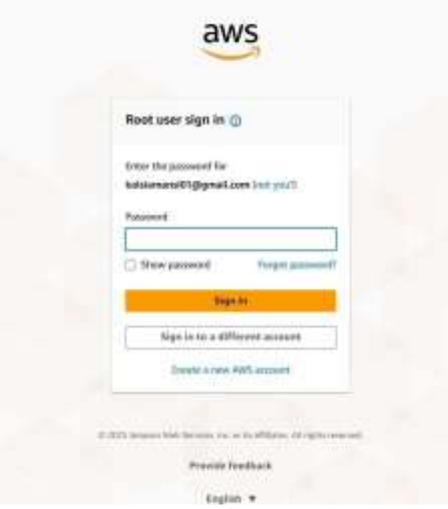
Activity Completed.

PRACTICAL- 8

Aim: Deploying of Node Js Application on Elastic Beanstalk Service

PROCEDURE:

Step 1: Sign in to AWS Console with your root credentials.



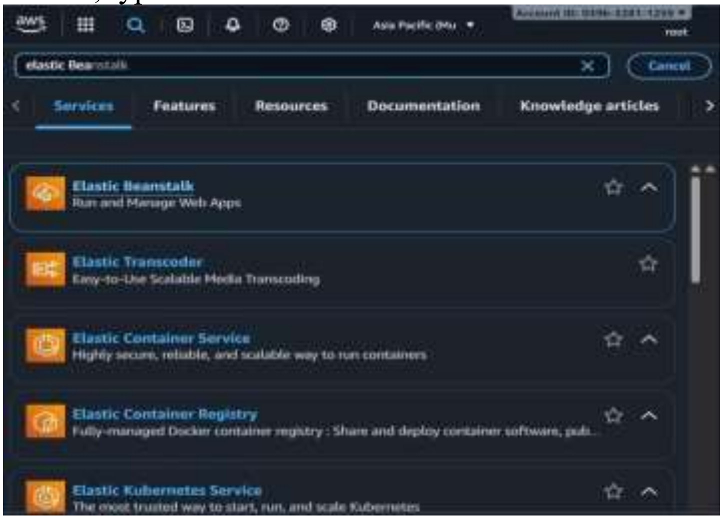
Root user sign in

Enter the password for [illegible]@gmail.com

Password

□ Show password   Forgot password?

Step 2: In the AWS search bar, type **Elastic Beanstalk** and click on it.



elastic Beanstalk

Elastic Beanstalk
Run and Manage Web Apps

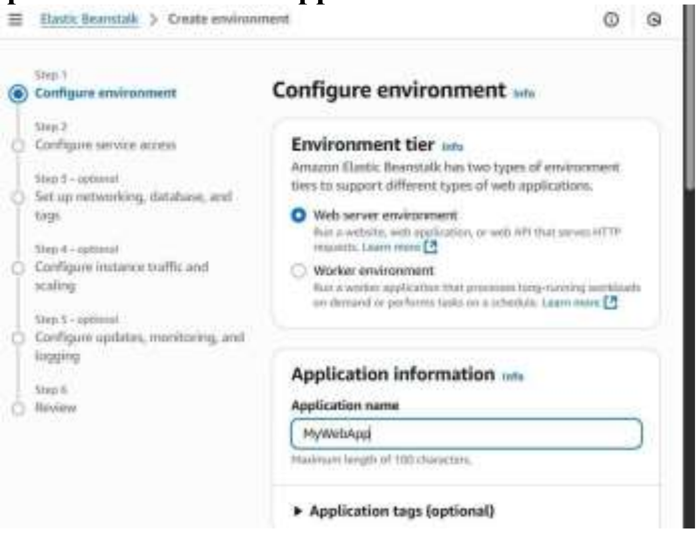
Elastic Transcoder
Easy-to-Use Scalable Media Transcoding

Elastic Container Service
Highly secure, reliable, and scalable way to run containers

Elastic Container Registry
Fully-managed Docker container registry : Share and deploy container software, pub...

Elastic Kubernetes Service
The most trusted way to start, run, and scale Kubernetes

Step 3: Click **Create Application**. Fill in the **Application Name**.



Elastic Beanstalk > Create environment
Step 1
Configure environment
Step 2
Configure service access
Step 3 - optional
Set up networking, database, and tags
Step 4 - optional
Configure instance traffic and scaling
Step 5 - optional
Configure updates, monitoring, and logging
Step 6
Review

Configure environment

Environment tier

Amazon Elastic Beanstalk has two types of environment tiers to support different types of web applications.

● Web server environment
Run a website, web application, or web API that serves HTTP requests. Learn more

○ Worker environment
Run a worker application that processes long-running workloads on demand or performs tasks on a schedule. Learn more

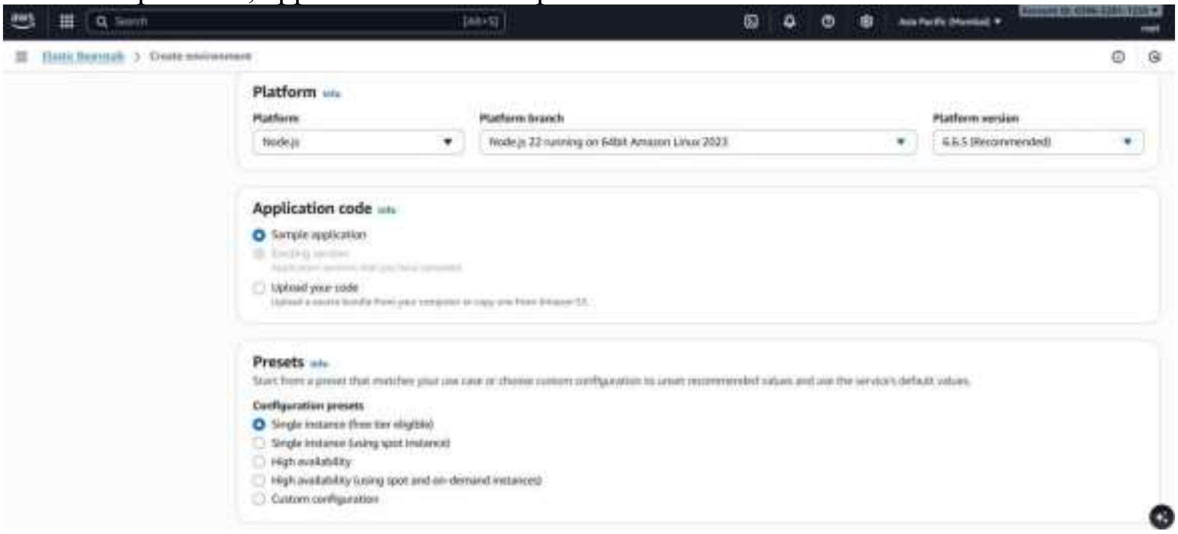
Application information

Application name: MyWebApp

Maximum length of 100 characters.

▸ Application tags (optional)

Step 4: Choose platform, application code and presets.



Elastic Beanstalk > Create environment

Platform

Platform: Node.js

Platform branch: Node.js 22 running on 64bit Amazon Linux 2023

Platform version: 6.6.5 (Recommended)

Application code

● Sample application

○ Existing version

○ Upload your code

Presets

Configuration presets

● Single instance (free tier eligible)

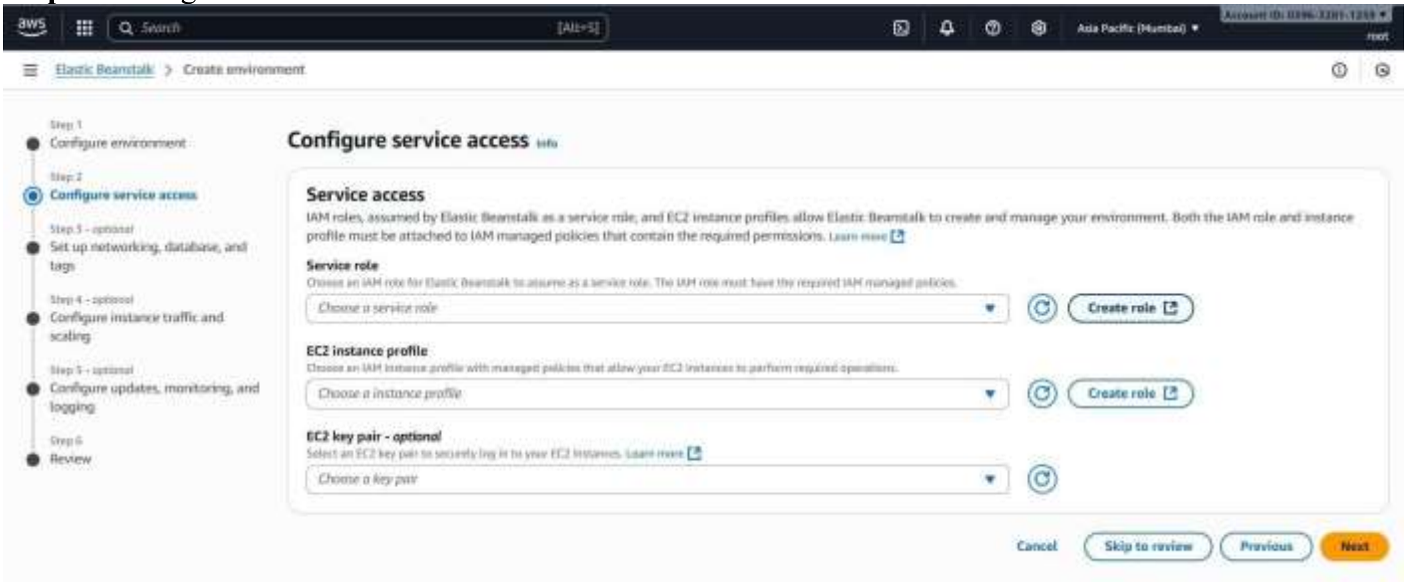
○ Single instance (using spot instance)

○ High availability

○ High availability (using spot and on-demand instances)

○ Custom configuration

Step 5: Configure Service-access .



Elastic Beanstalk > Create environment

Step 1 Configure environment

Step 2 Configure service access

Step 3 - optional Set up networking, database, and tags

Step 4 - optional Configure instance traffic and scaling

Step 5 - optional Configure updates, monitoring, and logging

Step 6 Review

Configure service access

Service access

IAM roles, assumed by Elastic Beanstalk as a service role, and EC2 instance profiles allow Elastic Beanstalk to create and manage your environment. Both the IAM role and instance profile must be attached to IAM managed policies that contain the required permissions. Learn more

Service role

Choose an IAM role for Elastic Beanstalk to assume as a service role. The IAM role must have the required IAM managed policies.

Choose a service role

EC2 instance profile

Choose an IAM instance profile with managed policies that allow your EC2 instances to perform required operations.

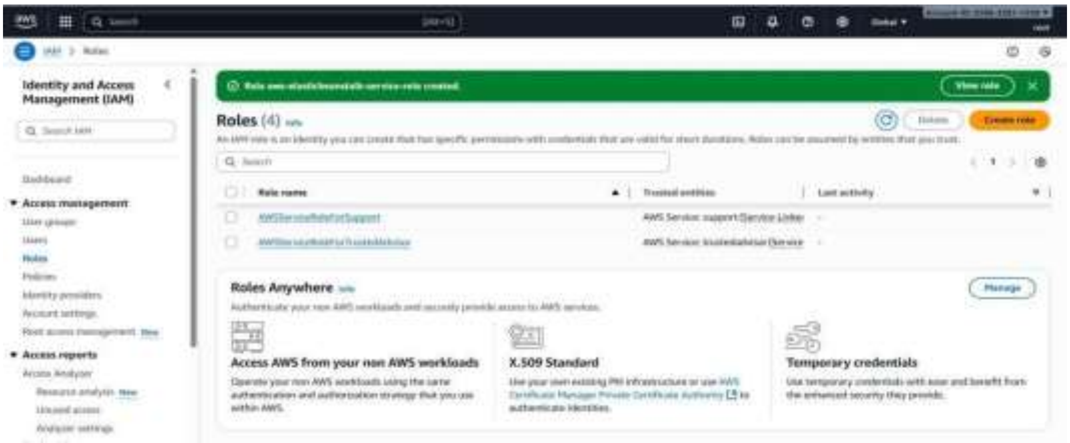
Choose a instance profile

EC2 key pair - optional

Select an EC2 key pair to securely log in to your EC2 instances. Learn more

Choose a key pair

Step 6: Create service role.



IAM > Roles

Role aws-elasticbeanstalk-service-role created.

Roles (4)

Role name	Trusted entities	Last activity
AWSServiceRoleForSupport	AWS Service: support (Service-Linked	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service	-

Roles Anywhere

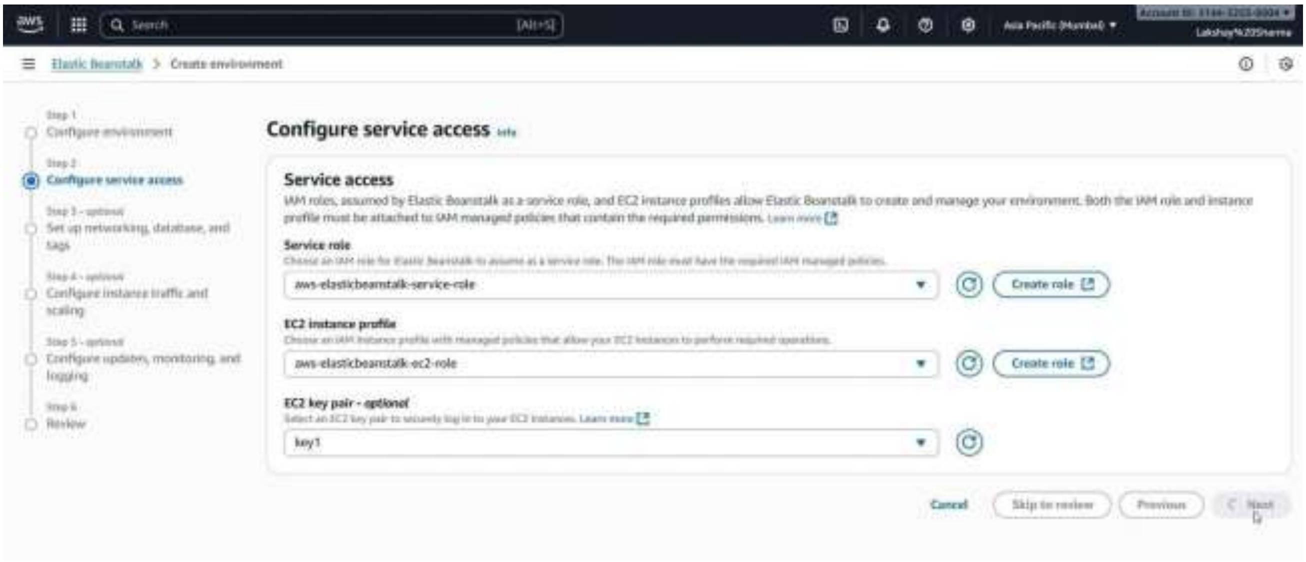
Authenticate your non AWS workloads and securely provide access to AWS services.

Access AWS from your non AWS workloads

X.509 Standard

Temporary credentials

Step 7: Configured service access.



Elastic Beanstalk > Create environment

Step 1
Configure environment

Step 2
Configure service access

Step 3 - optional
Set up networking, database, and tags

Step 4 - optional
Configure instance traffic and scaling

Step 5 - optional
Configure updates, monitoring, and logging

Step 6
Review

Configure service access

Service access

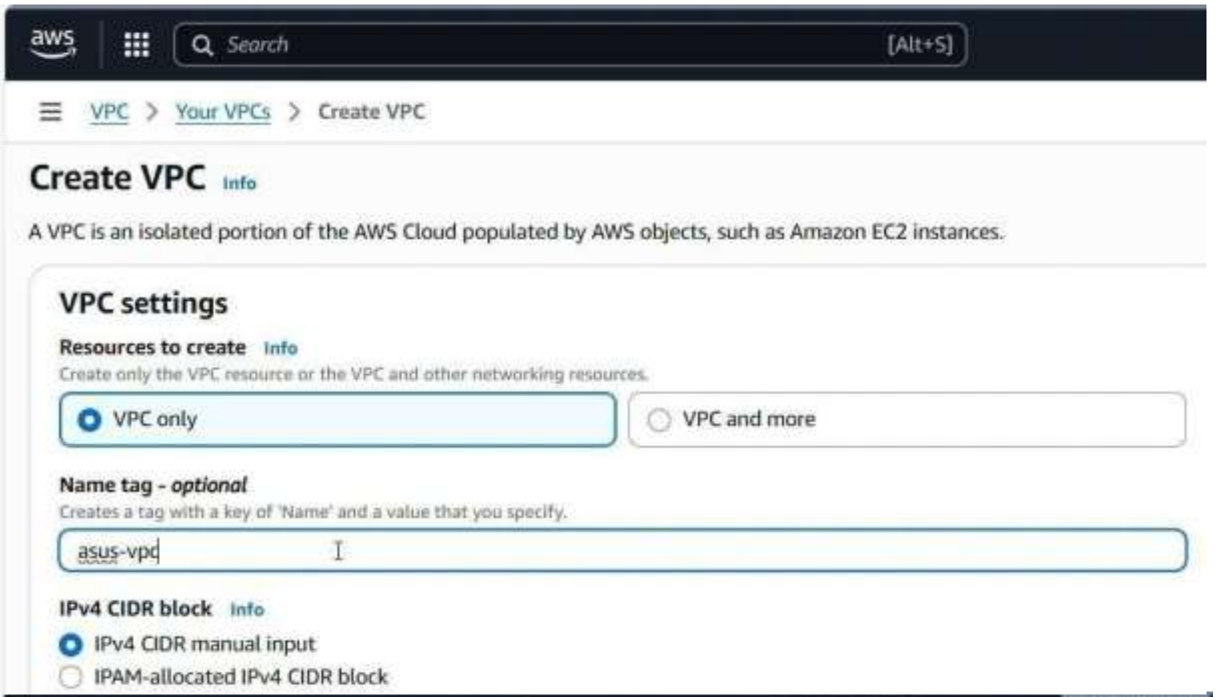
IAM roles, assumed by Elastic Beanstalk as a service role, and EC2 instance profiles allow Elastic Beanstalk to create and manage your environment. Both the IAM role and instance profile must be attached to IAM managed policies that contain the required permissions.

Service role: aws-elasticbeanstalk-service-role

EC2 instance profile: aws-elasticbeanstalk-ec2-role

EC2 key pair - optional: key1

Step 8: Create a VPC



VPC > Your VPCs > Create VPC

Create VPC

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

VPC settings

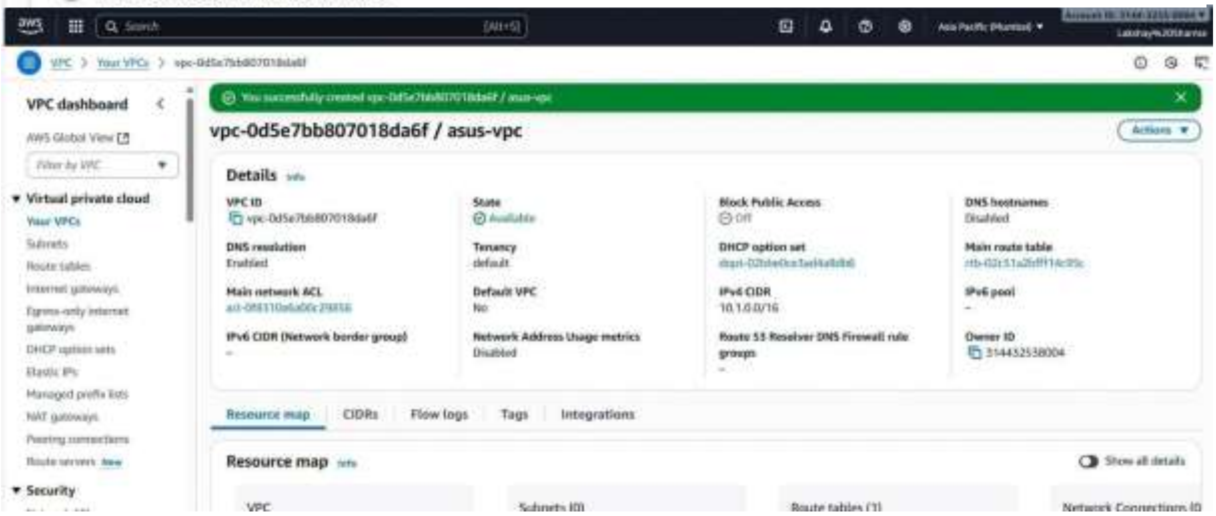
Resources to create
Create only the VPC resource or the VPC and other networking resources.

● VPC only ○ VPC and more

Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify.

asus-vpc

IPv4 CIDR block
● IPv4 CIDR manual input
○ IPAM-allocated IPv4 CIDR block



VPC > Your VPCs > vpc-0d5e7bb807018da6f

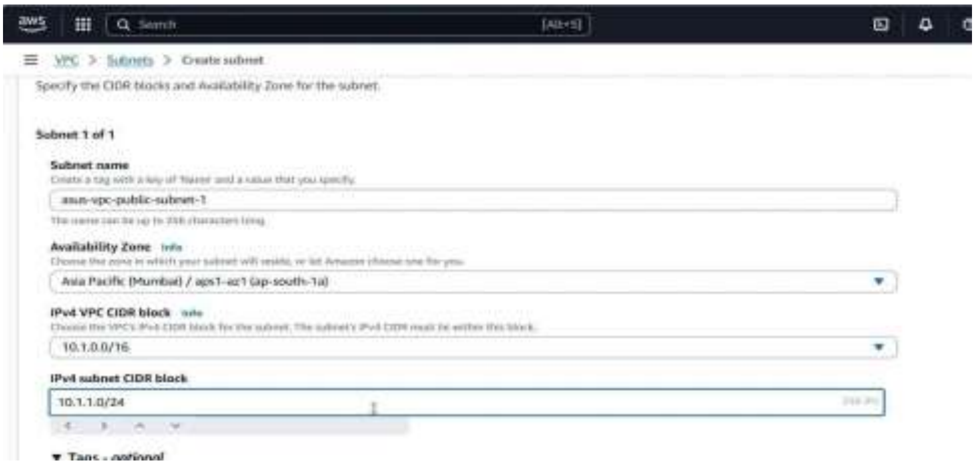
You successfully created vpc-0d5e7bb807018da6f / asus-vpc

vpc-0d5e7bb807018da6f / asus-vpc

Details

VPC ID vpc-0d5e7bb807018da6f	State Available	Block Public Access Off	DNS hostnames Disabled
DNS resolution Enabled	Tenancy default	DHCP option set [illegible]	Main route table [illegible]
Main network ACL [illegible]	Default VPC No	IPv4 CIDR 10.1.0.0/16	IPv6 pool –
IPv6 CIDR (Network border group) –	Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups –	Owner ID 314432538004

Step 9: Create Subnets.



VPC > Subnets > Create subnet

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name: asus-vpc-public-subnet-1

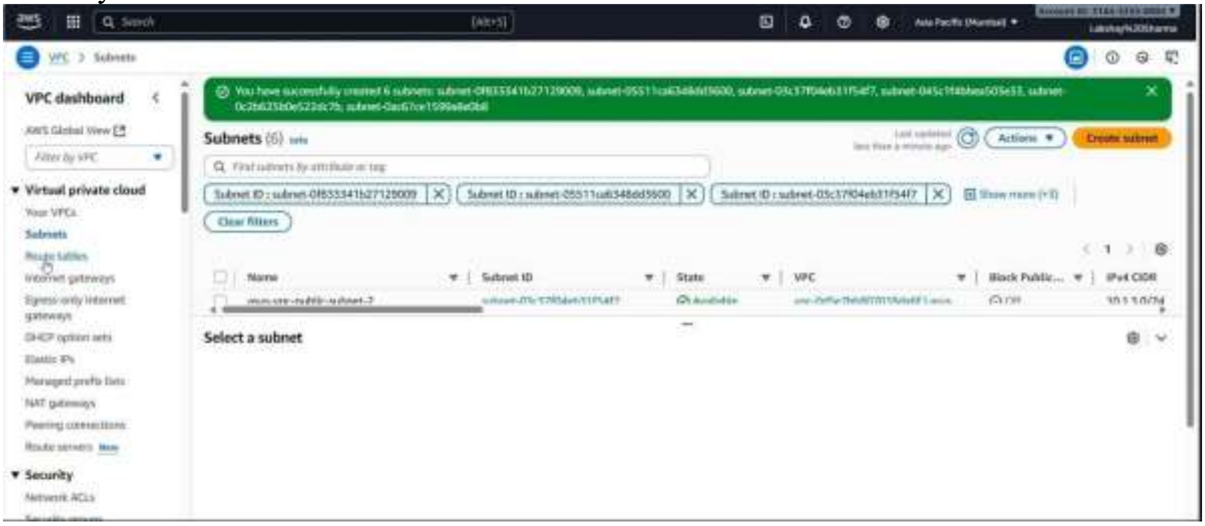
Availability Zone: Asia Pacific (Mumbai) / aps1-az1 (ap-south-1a)

IPv4 VPC CIDR block: 10.1.0.0/16

IPv4 subnet CIDR block: 10.1.1.0/24

▼ Tags - optional

Step 10: Similarly Create 6 Subnets.



You have successfully created 6 subnets: subnet-0f833341b27129009, subnet-05511ca6348dd5600, subnet-03c37f04eb31f54f7, subnet-045c1f4bbea505e53, subnet-0c2b6235b0e5223dc7b, subnet-0ac67ce1599a8e0b8

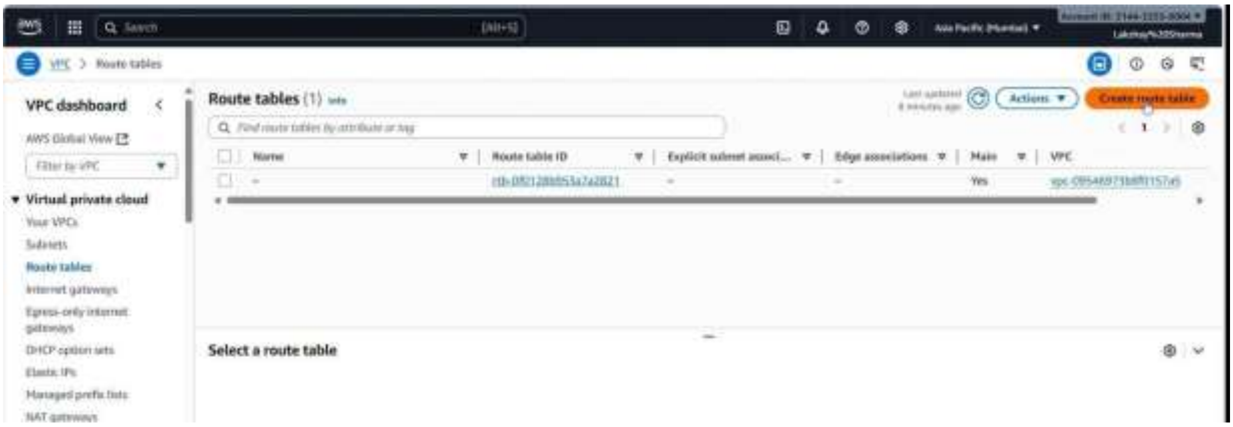
Subnets (6)

Subnet ID : subnet-0f833341b27129009 | Subnet ID : subnet-05511ca6348dd5600 | Subnet ID : subnet-03c37f04eb31f54f7

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR
asus-vpc-public-subnet-2	subnet-03c37f04eb31f54f7	Available	[illegible]	Off	10.1.3.0/24

Select a subnet

Step 11: Create route tables.

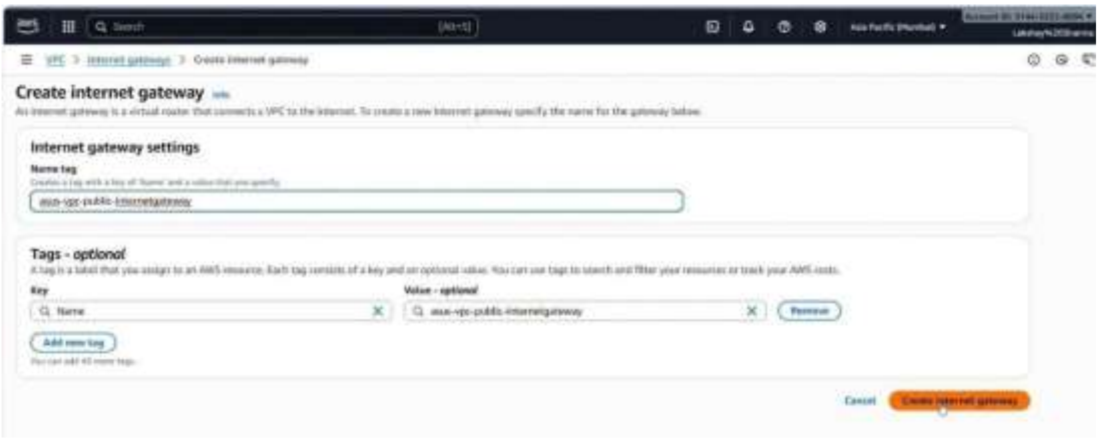


Route tables (1)

Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC
-	rtb-0f0128b053a7a2821	-	-	Yes	vpc-0954697...

Select a route table

Step 12: Create internet gateway.



Create internet gateway Info

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag

Creates a tag with a key of 'Name' and a value that you specify.

asus-vpc-public-internetgateway

Tags - optional

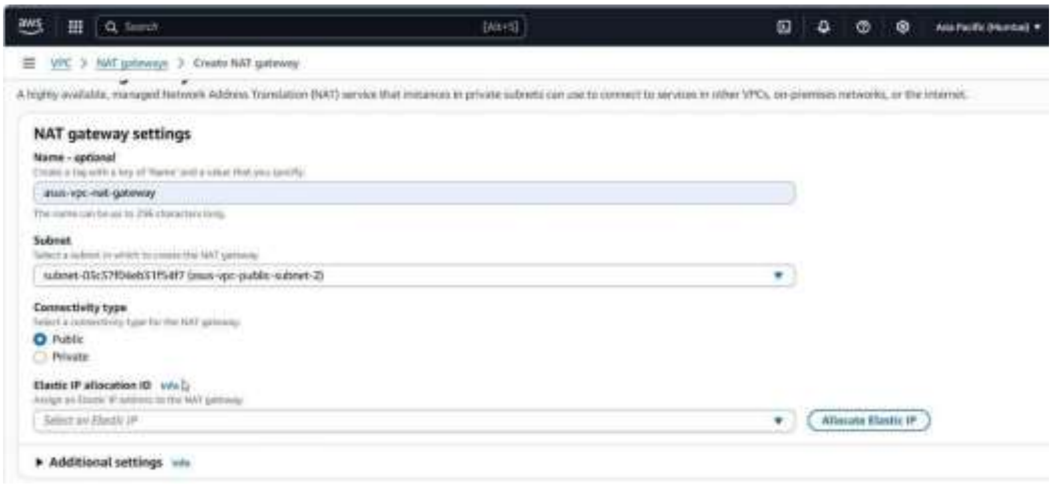
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key: Name

Value - optional: asus-vpc-public-internetgateway

You can add 49 more tags.

Step 13: Create NAT gateway.



A highly available, managed Network Address Translation (NAT) service that instances in private subnets can use to connect to services in other VPCs, on-premises networks, or the internet.

NAT gateway settings

Name - optional

Creates a tag with a key of 'Name' and a value that you specify.

asus-vpc-nat-gateway

The name can be up to 256 characters long.

Subnet

Select a subnet in which to create the NAT gateway.

subnet-05c57f04eb51f54f7 (asus-vpc-public-subnet-2)

Connectivity type

Select a connectivity type for the NAT gateway.

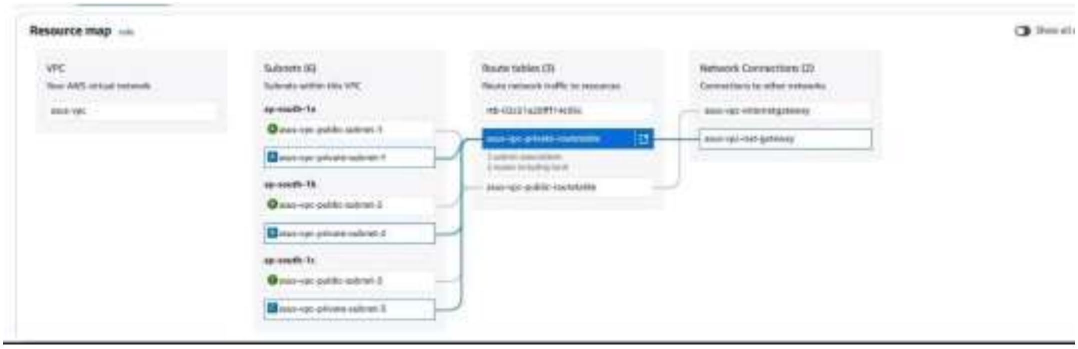
● Public

○ Private

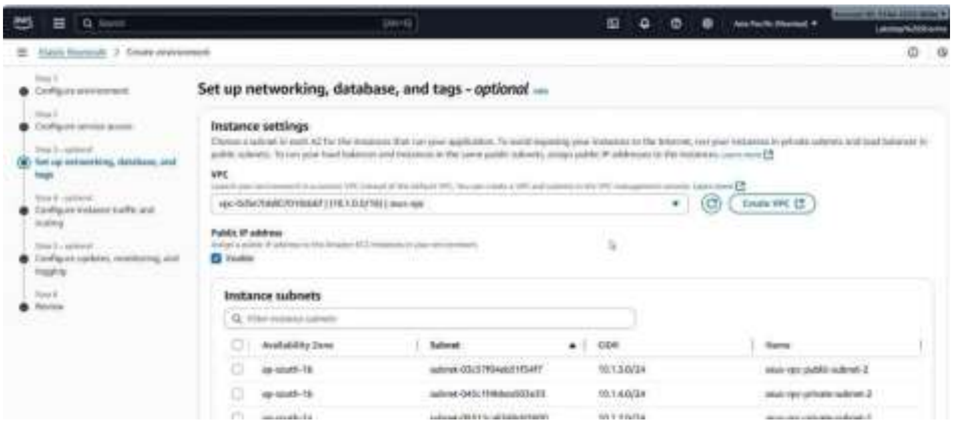
Elastic IP allocation ID Info

Assign an Elastic IP address to the NAT gateway.

Select an Elastic IP



Step 14: Set up networking,database,and tags.



Set up networking, database, and tags - *optional*

Instance settings

VPC

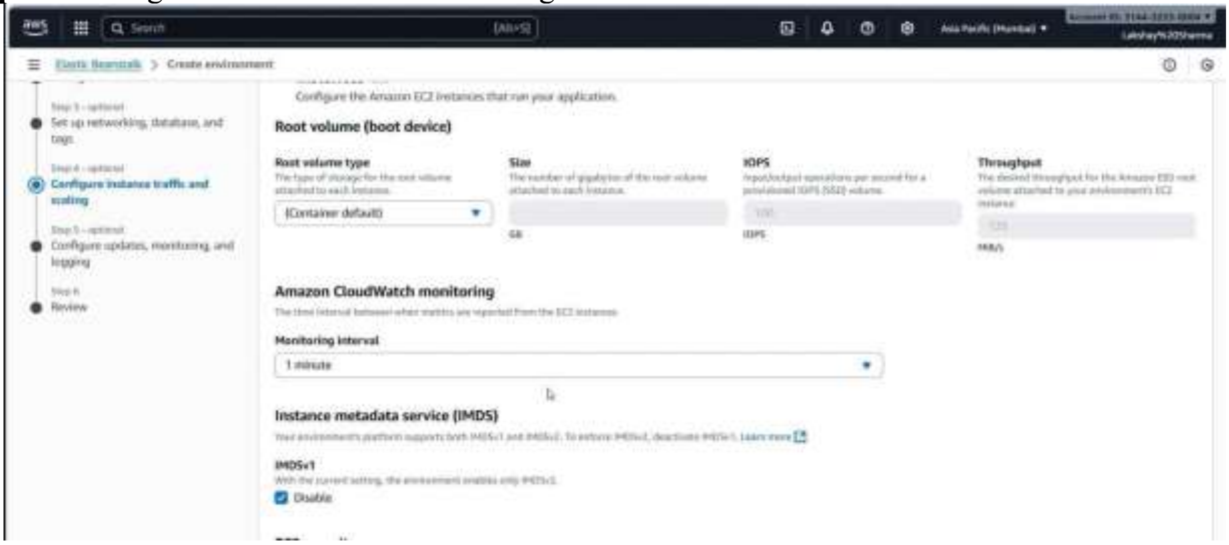
Public IP address

☑ Enable

Instance subnets

	Availability Zone	Subnet	CIDR	Name
□	ap-south-1b	[illegible]	10.1.3.0/24	[illegible]
□	ap-south-1b	[illegible]	10.1.4.0/24	[illegible]

Step 15: Configure instance traffic and scaling.



Configure the Amazon EC2 instances that run your application.

Root volume (boot device)

Root volume type: (Container default)

Size: GB

IOPS: IOPS

Throughput: MB/s

Amazon CloudWatch monitoring

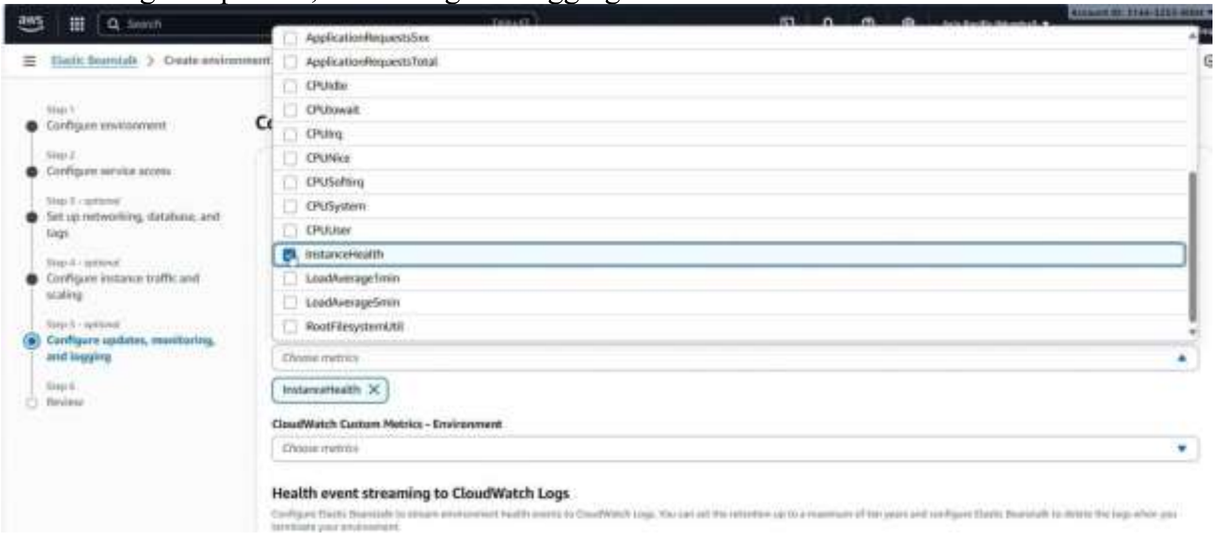
Monitoring interval: 1 minute

Instance metadata service (IMDS)

IMDSv1

☑ Disable

Step 16: Configure updates ,monitoring and logging.



□ ApplicationRequests5xx
□ ApplicationRequestsTotal
□ CPUIdle
□ CPUIowait
□ CPUIrq
□ CPUNice
□ CPUSoftirq
□ CPUSystem
□ CPUUser
☑ InstanceHealth
□ LoadAverage1min
□ LoadAverage5min
□ RootFilesystemUtil

Choose metrics

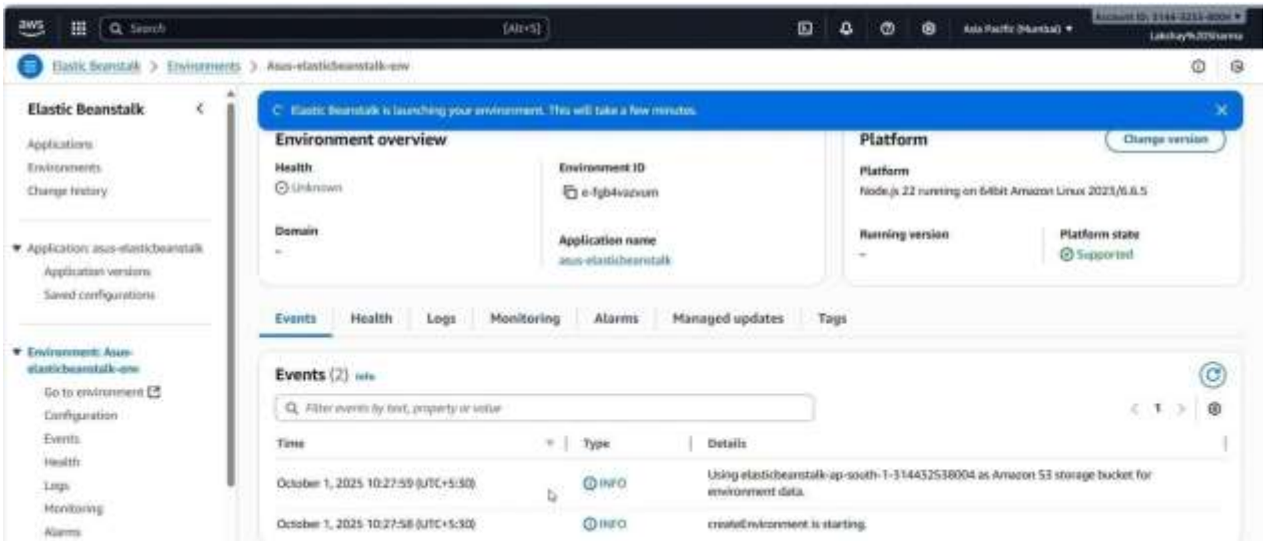
InstanceHealth ✕

CloudWatch Custom Metrics - Environment

Choose metrics

Health event streaming to CloudWatch Logs

Step 17: Review then create.



Elastic Beanstalk is launching your environment. This will take a few minutes.

Environment overview

Health: Unknown

Environment ID: e-fgb4vazvum

Domain: -

Application name: asus-elasticbeanstalk

Platform

Platform: Node.js 22 running on 64bit Amazon Linux 2023/6.6.5

Running version: -

Platform state: Supported

Events (2)

Time	Type	Details
October 1, 2025 10:27:59 (UTC+5:30)	INFO	Using elasticbeanstalk-ap-south-1-314432538004 as Amazon S3 storage bucket for environment data.
October 1, 2025 10:27:58 (UTC+5:30)	INFO	createEnvironment is starting.

Conclusion:

In this experiment, we learned how to **deploy and manage applications using Elastic Beanstalk**. We created an environment, selected the platform and application code, and accessed the deployed app through a URL. This experiment demonstrated how Elastic Beanstalk **automates infrastructure management** (like EC2, load balancers, and scaling) so developers can focus on application code rather than server setup.